SECURITY OF HEALTHCARE.GOV

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 19, 2013

Serial No. 113–100

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

87–764 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

TIM MURPHY, Pennsylvania
Chairman

MICHAEL C. BURGESS, Texas
Vice Chairman
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
GREGG HARPER, Mississippi
PETE OLSON, Texas
CORY GARDNER, Colorado
H. MORGAN GRIFFITH, Virginia
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
BRUCE L. BRALEY, Iowa
BEN RAY LUJAN, New Mexico
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
KATHY CASTOR, Florida
PETER WELCH, Vermont
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
GENE GREEN, Texas
JOHN D. DINGELL, Michigan *(ex officio)*
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

SECURITY OF HEALTHCARE.GOV

TUESDAY, NOVEMBER 19, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:15 a.m., in room 2123 of the Rayburn House Office Building, Hon. Tim Murphy (chairman of the subcommittee) presiding.

Members present: Representatives Murphy, Burgess, Blackburn, Scalise, Harper, Olson, Gardner, Griffith, Johnson, Long, Ellmers, Barton, Upton (ex officio), DeGette, Braley, Lujan, Schakowsky, Butterfield, Welch, Tonko, Yarmuth, Dingell, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight; Mike Bloomquist, General Counsel; Sean Bonyun, Communications Director; Karen Christian, Chief Counsel, Oversight and Investigations; Noelle Clemente, Press Secretary; Brad Grantz, Policy Coordinator, Oversight and Investigations; Brittany Havens, Legislative Clerk; Sean Hayes, Counsel, Oversight and Investigations; Brandon Mooney, Professional Staff Member; Andrew Powaleny, Deputy Press Secretary; Tom Wilbur, Digital Media Advisor; Jessica Wilkerson, Staff Assistant; Stacia Cardille, Democratic Deputy Chief Counsel; Brian Cohen, Democratic Staff Director, Oversight and Investigations, and Senior Policy Advisor; Hannah Green, Democratic Staff Assistant; Elizabeth Letter, Democratic Press Secretary; Karen Lightfoot, Democratic Communications Director and Senior Policy Advisor; Karen Nelson, Democratic Deputy Committee Staff Director for Health; Stephen Salsbury, Democratic Special Assistant; and Matt Siegler, Democratic Counsel.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Good morning. I convene this hearing of the Subcommittee on Oversight and Investigations to discuss the security of the Healthcare.gov Web site.

Americans want to know the answers to two simple questions: is my information secure if I use Healthcare.gov, and why should I believe the administration that it is?

It has been nearly 50 days since the launch of Healthcare.gov, and the Web site is still not functioning at an acceptable level. This is despite the numerous promises and assurances the public was

given by members of the administration leading up to and over the several months up to the launch of the Web site.

This committee heard directly from Secretary Sebelius, Administrator Tavenner, and CCIIO Director, Gary Cohen, that they were ready by October 1. We are all deeply troubled that the individuals who want to be in charge of America's healthcare system could not even predict accurately if the Web site would work. And those predictions were not just limited to the Web site. We have also been routinely promised that the Web site was safe, and that Americans' personal information would be secure.

When Administrator Tavenner last appeared before this committee, she informed us that testing began in October of last year, that end-to-end testing would be completed by the end of August this year. We have now learned that this simply was not the case. End-to-end testing is not possible when the Web site isn't completed.

Today we hope to hear from our witness about how much of the Web site remains to be built. If the first parts of Healthcare.gov have been this problematic, we are obviously concerned about parts that are being constructed under current pressures and time constraints.

The witness for our first panel today is Mr. Henry Chao, the Deputy Chief Information Officer at the Centers for Medicare and Medicaid Services, and we want to thank you for coming and testifying today. I can only imagine how stressful the last few months have been for you, so welcome here. Yet, I hope you can appreciate the fact that HHS has a ways to go to regain the trust of the American people in this Web site. They were promised a functioning Web site as easy as buying a TV on Amazon, and what they got was a train wreck.

The reason the trust of the American people may be so difficult to regain is because every day, new revelations emerge that show this wreck was entirely foreseeable. Last week, this subcommittee uncovered emails from CMS showing that as early as July of this year, Mr. Chao, our first witness, was worried that the company primarily responsible for building the Web site, CGI, would "crash at takeoff."

Today this subcommittee also released materials showing that as early as March to April of this year, top administration officials were well aware that Healthcare.gov was far off schedule, and testing of the Web site would be limited. We have also learned that Healthcare.gov was only launched after Administrator Tavenner signed an authority to operate, which included a memo warning her that a full security control assessment was not yet completed. This memo makes it clear that the highest levels of CMS knew that there were security risks present, yet again, while this document was being signed in private, administration officials were promising the public that in only a few days, the American people would be able to use a perfectly functioning Web site.

A few weeks ago, Secretary Sebelius told this committee that the highest security standards are in place, and people have every right to expect privacy. I hope that today we hear what those standards are, not only from Mr. Chao and also from our second panel as well.

Our second panel features some of the contractors that are responsible for the security of Healthcare.gov, and I thank them for testifying today. I am disappointed that one of the companies responsible for security, Verizon, chose not to testify today. We will certainly be following up with Verizon so that they are accountable to the public for their work here.

Today's hearing is not just about the Web site. Web sites can be fixed. What cannot be fixed is the damage that could be done to the American people if their personal data is compromised. Right now, Healthcare.gov screams to those who are trying to break into the system, "If you like my healthcare info, maybe you can steal it."

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF HON. TIM MURPHY

Americans want to know the answers to two simple questions: Is my information secure if I use HealthCare.gov? And why should I believe the administration that it is?

It has been nearly 50 days since the launch of HealthCare.gov, and the Web site is still not functioning at an acceptable level. This is despite the numerous promises and assurances the public was given by members of the administration leading up to the launch of the Web site. This committee heard directly from Secretary Sebelius, Administrator Tavenner, and CCIIO Director Gary Cohen that they were ready by October 1. We are all deeply troubled that the individuals who want to be in charge of America's healthcare system could not even predict accurately if the Web site would work.

And those predications were not just limited to the Web site. We have also been routinely promised that the Web site was safe and that Americans personal information would be secure. When Administrator Tavenner last appeared before this committee, she informed us that testing began in October of last year, and that end-to-end testing would be completed by the end of August this year. We have now learned that this was simply not the case. End-to-end testing is not possible when the Web site isn't completed. Today, we hope to hear from our witness about how much of the Web site remains to be built. If the first parts of HealthCare.gov have been this problematic, we are obviously concerned about parts that are being constructed under current pressures and time constraints.

The witness for our first panel today is Mr. Henry Chao, the Deputy Chief Information Officer at the Centers for Medicare and Medicaid Services. We thank you for testifying today. I can only imagine how stressful the last few months have been. Yet, I hope you can appreciate the fact that HHS has a ways to go to regain the trust of the American people. They were promised a functioning Web site—as easy as buying "a TV on Amazon"—and they got a train wreck.

The reason the trust of the American people may be so difficult to regain is because every day new revelations emerge that show this train wreck was entirely foreseeable. Last week this subcommittee uncovered emails from CMS showing that as early as July of this year Mr. Chao, our first witness, was worried that the company primarily responsible for building the Web site—CGI—would crash on takeoff. This subcommittee also released materials showing that as early as April top administration officials were well aware that Healthcare.gov was far off schedule and testing of the Web site would be limited.

We have also learned that HealthCare.gov was only launched after Administrator Tavenner signed an "Authority to Operate," which included a memo warning her that a full Security Control Assessment was not completed. This memo makes it clear that the highest levels of CMS knew that there were security risks present. Yet, again, while this document was being signed behind closed doors, in public, administration officials were promising that in only a few days the public would be able to use a perfectly functioning Web site.

A few weeks ago Secretary Sebelius told this committee that the "highest security standards are in place, and people have every right to expect privacy." I hope that today we hear what those standards are from not only Mr. Chao, but our second panel as well. Our second panel features some of the contractors that are responsible for the security of HealthCare.gov, and I thank them for testifying today. I am disappointed that one of the companies responsible for security, Verizon, chose not

to testify today. We will certainly be following up with Verizon so that they are accountable to the public for their work here.

Today's hearing is not just about the Web site. Web sites can be fixed. What cannot be fixed is the damage that could be done to Americans if their personal data is compromised.

Right now, HealthCare.gov screams to crooks, "If you like my healthcare info, you can steal it."

Mr. MURPHY. But I now recognize for an opening statement Ms. DeGette of Colorado, for 5 minutes.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you very much, Chairman Murphy. I want to add to your thanks to Mr. Chao for being here today, as well as the three contractor witnesses; MITRE, CCSi and Foreground.

We must make sure that the data on Healthcare.gov is secure. Everybody can agree on that. The American people must know that their data is protected when they go on the site to find a quality, affordable insurance plan for themselves or their families. This is critical. However, my fear is that today's hearing is actually less about the facts of the security of Healthcare.gov, and more about political points and undermining the ACA.

Now, without a doubt, no one could disagree there are troubling problems with the rollout of the Exchanges. Three weeks ago, our full committee held the first hearing on the inexcusable fact that Healthcare.gov seems to have been broken since it was very first launched. And three weeks later, while improving, it is clearly not up to speed. As I have said before, the Exchanges need to be fixed, and they need to be fixed fast so that the American people can easily access quality, affordable insurance plans open to them. I hope we will have another hearing after the November 30 deadline to see how they are working.

My fear about this hearing today though is that it won't enlighten the American public, but instead raise unjustified fears about security piling on all of the other issues. Now, obviously, as I said, we need to make sure that the data on Healthcare.gov is secure, but we should not create smoke if there is no fire.

So before we begin, I want to give the American people some peace of mind based on the facts that we know about security on Healthcare.gov.

First, and critically, no American has to provide any personal health information to Healthcare.gov or to insurers in order to qualify for health coverage and subsidies. To make sure about this, I went on the Exchange myself the other day, and that is because the ACA bans discrimination based on pre-existing health conditions. Before the ACA became law, Americans buying coverage on the individual insurance market had to fill out page after page of personal health information to apply for insurance. But no longer, thanks to the Affordable Care Act. Americans do not have to turn over any private health insurance to get coverage.

Second, while no Web site in the Government or in the private sector is 100 percent secure, unfortunately, there is a complex and detailed set of rules that HHS must follow to make sure that data

on Healthcare.gov is secure. And I am looking forward to hearing from you, Mr. Chao, about these security issues today.

The Agency has a long record of maintaining personal information about Medicare, Medicaid, Social Security and many areas, and has never had a significant leak of information. HHS must comply with the Federal Information Security Management Act, and National Institute of Standards and Technology Guidelines to protect information systems and the data collected or maintained by Healthcare.gov. And like all Federal agencies, HHS is required to develop, document and implement an agency-wide information security program.

To date, our committee's investigation has found that CMS has complied with every important security rule and guideline. They hired a small army of contractors to make sure the Web site is secure, and they are going to talk to us about it today.

The memo, Mr. Chairman, that you talked about at our last hearing, that identified some security concerns, primarily a lack of end-to-end testing on Healthcare.gov, but it also outlined a mitigation plan, one we learned was—that the Agency was following to mitigate security risks. So I want to hear from the contractors and from you, Mr. Chao, if, in fact, these findings are being heeded.

Now, unfortunately, Mr. Chairman, I have to raise one more issue in my remaining minute, and that is this committee's grand tradition of bipartisanship investigation. Apparently, the committee, last Thursday, received a memo from CMS, Red Team discussion document. The majority on this committee did not share this memo with the minority on this committee until yesterday, coincidentally, just after they leaked this memo to The Washington Post. Now—and if you saw The Washington Post front page today, you saw a big story, and, Mr. Chairman, you were quoted in that story, talking about concerns about the readiness of the Exchange based on this memo.

I know that is not the topic of this hearing today, but I have got to say it is not in the tradition of the committee to conduct investigations that way. And when the majority received this memo, it should have immediately provided it to all of the members so that we could read it and find out. We are all just as concerned about making these Exchanges work.

And to that end, Mr. Waxman and I have written a letter expressing our displeasure, and we would like to enter that into the record at this time, Mr. Chairman.

[The information follows:]

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

November 19, 2013

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Upton and Chairman Murphy:

We are writing to express our extreme disappointment in the process by which you are conducting the Committee investigation into the readiness and security of Healthcare.gov.

We have learned that the Republican majority received documents and information related to the investigation on Thursday, November 14, 2013, from a subcontractor hired by Centers for Medicare and Medicaid Services to conduct a March 2013 "pressure test" of the "trajectory of the federal marketplace."[1] These documents were provided based on a request that was an outgrowth of an official Chairman's request letter sent on October 31, 2013.[2]

Republican Committee staff did not provide any documents to the Democratic staff until four days after they were provided to the Committee. At this point, minority staff was provided with only a partial production of these materials on Monday afternoon, November 18, less than 24 hours before today's hearing. Additional portions of this official document production were

---

[1] McKinsey & Company, *Red Team: Discussion document* (undated).

[2] Letter from Chairman Fred Upton, Chairman Emeritus Joe Barton, Chairman Tim Murphy, Chairman Joseph Pitts, Vice Chairman Marsha Blackburn, Vice Chairman Michael Burgess, Rep. Mike Rogers, and Rep. Bill Johnson to MITRE Corporation (Oct. 31, 2013).

withheld from the minority and appear to have been shared with press prior to being shared with minority Committee staff.

Your failure to provide the minority with copies of relevant investigatory documents in a timely fashion runs counter to the longstanding practice of this Committee. It is also inconsistent with House Rule XI, which provides that "all committee records (including hearings, data, charts and files) ... shall be the property of the House and each Member, Delegate and the Resident Commissioner shall have access thereto."[3] Additionally, the Rules prescribe that the ranking minority member "shall have access to information before a [investigative] subcommittee with which they so consult."[4]

Excluding Democratic members from timely access to the full Committee record calls into question the credibility and fairness of the Committee's inquiry.

We also observe that this is the second time in four days that you have leaked Committee investigative material to the press. Again, this is not the way the Committee traditionally operates, and we question your judgment in leaking this material without appropriate context, without the benefit of witness testimony to provide additional information, and in this latest case, without providing Democratic members timely access.

We urge you to reconsider your practices and ensure that Democratic members have access to the full Committee record in the future.

Sincerely,

Henry A. Waxman Diana DeGette John D. Dingell

[3] Rules of the House of Representatives, Rule XI clause (e)(2)(A).

[4] Rules of the House of Representatives, Rule XI clause (m)(C).

Mr. MURPHY. That is fine, and I will look forward to talking with you more about these procedures. I know that these came as part of a couple of hundred thousand pages of documents that we are going through, but I will be glad to review that with you because I certainly respect my colleague on this——

Ms. DEGETTE. That we were able to find it in time to give it to The Washington Post in time for today's hearing, and to be quoted——

Mr. MURPHY. We will——

Ms. DEGETTE [continuing]. In The Washington Post.

Mr. MURPHY. We will have a good discussion on that. I thank my colleague, whose time has expired.

I now recognize the chairman of the full committee, Mr. Upton, for 5 minutes.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, Mr. Chairman.

You know, for months, administration witnesses have come before this committee and assured us that the implementation of the President's healthcare law was "on track"—their words—and that Healthcare.gov would be ready for the October 1 launch. But why not give the straight story to the Congress and the public, because back on April 18, Secretary Sebelius testified in this very room, we have the Federal hub on track and on time. I can tell you we are on track. Those are her words. But we now know that the Secretary's testimony did not match what was happening behind the scenes.

Two weeks before she testified before this committee, Secretary Sebelius was present at an April 4 meeting where experts identified significant threats and risks launching the site on October 1. The administration was on track, on track for disaster, but stubbornly they stayed the course, repeating their claims that all is well and on track, right up until the mess that launched on October 1. And even after the launch, administration officials insisted that the volume was primarily the culprit, when they, in fact, knew otherwise.

But our oversight of the health law is not just about a Web site. No, it is not. It is about whether the public can trust and rely on this healthcare system that the administration has been building for over three years, and spending hundreds of millions of dollars. The failure of this Web site has significant consequences for all Americans. One important question is whether individuals will be able to enroll and obtain coverage by January 1. Security is another critical concern. How can the public trust a hastily thrown-together system in which meeting a deadline was more important for the administration than conducting complete end-to-end testing of the site's security.

Mr. Henry Chao, Deputy Chief Information Officer of CMS, is here to answer those questions, about CMS's management of the Federal Exchange and the implications for security. And, Mr. Chao, I do understand that you are a career employee, and have been at CMS for years, and I know, as Chairman Murphy indicated, the last few months have not been particularly easy. Last March, you

were one of the first to publicly offer a glimpse of the true situation when you candidly remarked about the Web site and said, let us just make sure it is not a Third World experience. Documents produced to the committee paint a clear picture that the administration officials, in fact, knew for months before the October 1 date about delays and problems with the Web site development. Mr. Chao, you have been responsible for managing the development of Healthcare.gov, but I can imagine many matters were outside of your control. And given the lack of end-to-end testing, I hope that you can explain to us today why the administration felt confident in the security of Healthcare.gov when the system went live on October 1.

We are also joined by three companies that were awarded contracts by CMS to provide security services for the Federal Exchange. These companies are here also today to answer questions about their roles. I know the subjects of security presents certain sensitivities, and I am glad that they made the decision to accept our invitations to testify and inform us about how Healthcare.gov works or doesn't.

One thing that we have learned; there are countless contractors involved in building this Web site, and responsibilities are divided. Very divided. It is a complex system, I know, but we would like to know how the delays and rushed implementation have affected or complicated the ability to perform the security work for the Web site.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

For months, administration witnesses have come before this committee and assured us thatimplementation of the president's healthcare law was "on track," and that HealthCare.gov would be ready for the October 1 launch.

But why not give the straight story to the Congress and the public? On April 18, Secretary Sebelius testified in this very room, "we have the Federal hub on track and on time. . I can tell you we are on track." But we now know that the secretary's testimony did not match what was happening behind the scenes. Two weeks before she testified before this committee, Secretary Sebelius was present at an April 4 meeting where experts identified significant threats and risks to launching the site on October 1. The administration was on track—on track for disaster. But stubbornly, they stayed the course, repeating their claims that all was well and on track right up until the mess that launched October 1. Even after the launch, administration officials insisted volume was the primary culprit, when they knew otherwise.

But our oversight of the health law is not just about a Web site. It is about whether the public can trust and rely on this healthcare system that the administration has been building for over 3 years. The failures of this Web site have significant consequences for Americans. One important question is whether individuals will be able to enroll and obtain coverage by January 1. Security is another critical concern. How can the public trust a hastily thrown together system in which meeting a deadline was more important for the administration than conducting complete, end to end testing of the site's security?

Mr. Henry Chao, Deputy Chief Information Officer of CMS, is here to answer our questions about CMS' management of the Federal exchange and the implications for security. Mr. Chao, I understand you are a career employee and have been at CMS for years. I am sure the last few months have not been easy for you. Last March, you were one of the first to publicly offer a glimpse of the true situation when you candidly remarked about the Web site, "Let's just make sure it's not a third-world experience." Documents produced to the committee paint a clearer picture that administration officials knew for months before October 1 about delays and problems with the Web site development. Mr. Chao, you have been responsible for managing the development of HealthCare.gov, but I imagine many matters were outside your control. Given the lack of end-to-end testing, I hope you can explain to us today why

the administration felt confident in the security of HealthCare.gov when the system went live on October 1.

We are also joined by three companies that were awarded contracts by CMS to provide security services for the Federal exchange. These companies—MITRE, CCSi, and Foreground—are here today to answer questions about their roles. I know the subject of security presents certain sensitivities and I am glad they made the decision to accept our invitations to testify and inform this committee about how HealthCare.gov works. One thing we have learned—there are countless contractors involved in building this Web site, and responsibilities are divided. It is a complex system. I would like to know how the delays and rushed implementation have affected or complicated your ability to perform the security work for the Web site.

Mr. UPTON. And I yield the balance of my time to Dr. Burgess.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. I thank the chairman for the recognition, and I do want to thank our witnesses for being here today.

Pretty broad agreement, the implementation of the Affordable Care Act has been problematic, and rather than getting better, it may be getting worse. We have low enrollment numbers, a Web site so bad that it has required the appointment of a glitch tsar, cancelled plan, broken promises from the President, just for starters. These initial problems break the surface of the deeper issues that lie ahead for not just the law, but for the American people that must live under the law.

And, Mr. Chao, you probably, prior to anyone else, sounded the alarm with that speech to AHIP, and I know you are tired of hearing it, but I will tell you once again, your comments that you were just trying to prevent the Web site from becoming a Third World experience, I admire your ability to see over the horizon and tell the problems before they come up and hit you in the windshield. But also you are the one who recommended that it was safe to launch the Web site on October 1. So what happened in those 6 months that led you, yourself, and others in the administration to believe that this law was, in fact, ready for primetime? Not only did the Center for Medicare and Medicaid Services fail to establish basic functionality, but Healthcare.gov's flaws continue to pose a threat to the security of Americans' personal data. And just on a personal note, when I went to Healthcare.gov this morning, it was still not functional. Another Web site, HealthSherpa.com, can actually tell me about the plans that are available in my area. We know it was possible to do this. We are all wondering why it wasn't.

Thank you, Mr. Chairman. I will yield back.

Mr. MURPHY. Gentleman yields back.

Now recognize the ranking member of the full committee, Mr. Waxman, for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you very much, Mr. Chairman.

The last 6 weeks have been difficult ones for supporters of the Affordable Care Act. The troubled rollout of the Web site prevented many of our constituents from signing up for the affordable, high-

quality coverage for which they now qualify. And it has been relentlessly exploited for political gain by Republican opponents of the law.

I was interested to hear the phrase in the 2 Republicans' statements, maybe in all of them; we don't want a Third World Web site. Well, let me tell you what is Third World. Third world in this country is when we leave millions of people unable to get insurance because they have pre-existing medical conditions, or they can't afford it. No other industrial country allows such a thing to happen, but that is what Republicans who have opposed this law would have us return to.

I think we are turning the corner on the Web site. On Friday, Jeff Zients, the administration's point person on Healthcare.gov, announced two key metrics of improvement, and it seems to me these are all very good signs the Web site is getting better. Additional improvements are still needed, but Healthcare.gov means more and more people will be signing up for coverage as that Web site becomes more usable.

I want to tell you what is happening in California. In the first month, 35,000 people enrolled in the Exchange, over 70,000 qualified for Medicaid, and State officials say that the pace of enrollment is increasing. In just the first 12 days of November, enrollment from the first month almost doubled.

Now, I know we are looking today at the issue of data security on Healthcare.gov. It is an important issue. We should begin by acknowledging that the ACA represents an enormous step forward for privacy because, when people apply for insurance coverage, the law bans them from being asked questions about their underwriting, about their medical conditions, about the privacy of things that affect their health, because it is not necessary to ask those questions. They are not going to be denied insurance coverage because of previous medical problems. But there is some personal information that people are going to be asked for when they sign up, and we need to ensure that this information is protected.

This question comes up repeatedly—came up repeatedly when Secretary Sebelius was before us. She told us the department is placing a high priority on the security of the Web site, and the highest security standards are in place to protect personal information on Healthcare.gov.

I hope this hearing will be serious, evenhanded inquiry, but I fear that some of my Republican colleagues may exaggerate security concerns to stoke public fear, and exaggerate it so that they can dissuade people from even signing up. This is exactly what this subcommittee did when they launched an investigation into nonprofit community organizations serving as healthcare navigators. They were harassing these people in order to prevent them from helping people learn what is available to them.

Mr. Chairman, yesterday we learned that you have been withholding important investigative documents, leaking them to the press before even providing them to the Democratic members and staff. And I sent you a letter this morning describing why this is a violation of the committee's precedent. It is not the way this committee has traditionally operated, and it raises concerns about

whether these hearings are becoming another partisan attempt to weaken the Affordable Care Act.

The committee should not go down that road. We should be using our oversight powers to improve the Affordable Care Act, not to sabotage it or to discourage Americans from signing up for quality care.

I want to yield the balance of my time, Mr. Chairman, to Mr. Dingell.

OPENING STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. DINGELL. I thank the gentleman. I ask unanimous consent to revise and extend my remarks, and I am pleased to be here and I am certainly pleased that my subscription to The Washington Post is in effect so I can find out what is being leaked by my Republican colleagues to the media.

This is interesting. We have clearly a violation of the practices, traditions and histories this committee and the investigations it has done. I speak as a member who has done more investigations than anybody in this room, including probably more than all of them put together.

Here, we have a breach of the responsibility of the leadership to make information available to the committee at the same time they make it to the press. I find that difficult, but worse than that, I find it intolerable that this committee is running around fishing for trouble where none exists. I feel a little bit like the old maid who came home and looked under the bed to find out if there was somebody there, hoping, in fact, that there would be. Unfortunately, there is not.

I have seen no evidence of any complaints or any evidence of misbehavior with regard to the information that is controlled by the Government. I would urge this committee to spend its time trying to make this situation work, and see to it that we collect the information that is necessary, make the Web site work, and see to it that we register the Americans so that we can cease being a Third World nation, both with regard to how the Congress runs and how the health care of this country works.

Mr. MURPHY. Gentleman's time has expired.

Mr. DINGELL. We are down around the Third World nations in the way that we take care of the health of our people. Look at the statistics.

Mr. MURPHY. Thank you.

Mr. DINGELL. It will give you a shock.

PREPARED STATEMENT OF HON. JOHN D. DINGELL

I thank the gentlemen for yielding.

Partisan politics have always been at the heart of the Majority's investigation into the Affordable Care Act, but today we have reached a new low.

Breaking with longstanding committee practice, the majority selectively released certain documents to the press before Democratic staff even had the opportunity to review.

Oversight is one of the most important responsibilities of the Congress, and it can result in good things when used properly. This committee has a long history of bipartisan cooperation when conducting oversight.

When I was chairman, the minority always had ample time to access documents. I hope we can soon return to that precedent and work on these issues together rather than playing games with the press.

Mr. MURPHY. Gentleman's time has expired.

Thank you very much. And now I would like to introduce the witnesses on our first panel for today's hearing. Henry Chao has served since January 2011 as the Deputy Chief Information Officer and Deputy Director of the Office of Information Services at the Centers for Medicare and Medicaid Services. Some of his prior roles include Chief Information Officer in the Office of Consumer Information and Insurance Oversight, and Chief Technology Officer for CMS. I will now swear in the witness.

You are aware, Mr. Chao, that the committee is holding an investigative hearing, and when doing so, has the practice of taking testimony under oath. Do you have any objection to taking testimony under oath? The witness indicates no. The Chair then advises you that under the rules of the House and the rules of the committee, you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony today? Mr. Chao indicates no. In that case, would you please rise, raise your right hand, I will swear you in.

[Witness sworn.]

Mr. MURPHY. Thank you. You are now under oath and subject to the penalties set forth in Title XVIII, Section 1001 of the United States Code. You may now give a 5-minute summary of your written statement. And make sure the microphone is on and pulled close to you. Thank you, Mr. Chao.

STATEMENT OF HENRY CHAO, DEPUTY CHIEF INFORMATION OFFICER AND DEPUTY DIRECTOR, OFFICE OF INFORMATION SERVICES, CENTERS FOR MEDICARE AND MEDICAID SERVICES

Mr. CHAO. Thank you, Chairman Murphy, Ranking Member DeGette, and members of the subcommittee for inviting me to testify about the security of the Federally Facilitated Marketplace.

The security and protection of personal and financial information is a top priority for CMS which, for decades, has protected the personal information of the more than 100 million Americans enrolled in Medicare, Medicaid and the Children's Health Insurance Program.

The protection of personal information in CMS programs is a monumental responsibility. Every day, CMS enrolls new Medicare beneficiaries, pays claims timely and efficiently, and protects the information of consumers and providers. CMS used this experience and our security-best practices to build a secure Federal Marketplace that consumers should feel confident entrusting with their personal information.

CMS follows Federal law, Government-wide security processes and standard business practices to ensure stringent security and privacy protections. CMS's security protections are not singular in nature; rather, the marketplace is protected by an extensive set of security layers.

First and foremost, the application—the online application is developed with secure code. Second, the application infrastructure is

physically and logically protected by our hosting provider. Third, the application is protected through an internet defense shield in order to protect unauthorized access to any personal data. Finally, several entities provide direct and indirect security monitoring, security testing, and security oversight which includes the various organizational groups that CMS are reporting to key stakeholders with respect to security and privacy.

This includes the Department of Health and Human Services. We also work in conjunction with US–CERT, which is operated by the Department of Homeland Security. CERT stands for Computer Emergency Response Team. And the Office of the Inspector General of HHS. Each of these groups has varying roles to ensure operational management and technical controls are implemented and successfully working.

The Federally Facilitated Marketplace is protected by the high standards demanded of Federal information systems, including regulations and standards proscribed by FISMA, NIST, the Privacy Act and the directives promulgated by the Office of Management and Budget.

CMS designed the marketplace IT systems and the Hub to reduce possible vulnerabilities and increase the efficiency. A large number of connections can cause security vulnerabilities. The Hub allows for 1 highly secured connection between highly protected databases of trusted State and Federal agencies, instead of hundreds of connections that would have been established as part of how normal business practices in present day in how Government connects organizations with each other to conduct business.

A series of business agreements enforce privacy controls between CMS and our Federal and State partners. Additionally, CMS designed the marketplace systems to limit the amount of personal data stored, and protects personal information and limits access through passwords, encryption technologies, zoned architecture with firewall separation in between the zones, and various other security controls to monitor log-in and to prevent unauthorized access to our systems.

CMS also protects the Federal Marketplace through intensive and stringent security testing. While the Federal Marketplace has had some performance issues that could have been addressed through more comprehensive functionality and performance testing, I want to be clear that we have conducted extensive security testing for the systems that went live on October 1. We continue to test for security on a daily and a weekly basis any new functions or code prior to its launch. Of course, we are working around the clock to fix our performance issues so that the vast majority of users have a smooth experience with the site by the end of the month.

While I cannot go into specifics of our security testing due to the sensitive nature, I assure you that CMS conducts continuous antivirus and malware scans, as well as monitors data flow and protections against threats by denying access to known source-bad IP addresses and actors. Additionally, we conduct two separate types of penetration testing on a weekly basis. The most recent penetration testing showed no significant findings. Also on a weekly basis, CMS reviews the operation system infrastructure and the

application software to be sure that these systems are compliant and do not have vulnerabilities. Vulnerabilities are often fixed immediately on-site, and retested to ensure the strength of our system's security. Each month, we review our plan of action and milestones in order to continuously improve our system's security.

For the Federally Facilitated Marketplace, we conduct security control assessments on a quarterly basis, which is beyond the FISMA requirements. As of today, no vulnerabilities identified by our tests have been exploited through an attack. Because of CMS's experience running trusted secure programs, our fulfillment of Federal security standards and constant and routine security monitoring and testing, the American people can be confident in the privacy and security of the marketplace.

Thank you, and I would be happy to answer your questions.

[The prepared statement of Mr. Chao follows:]

STATEMENT OF

HENRY CHAO

DEPUTY CHIEF INFORMATION OFFICER &
DEPUTY DIRECTOR, OFFICE OF INFORMATION SERVICES,
CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

SECURITY OF HEALTHCARE.GOV

BEFORE THE

U. S. HOUSE COMMITTEE ON ENERGY & COMMERCE, SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS

NOVEMBER 19, 2013

U. S. House Committee on Energy &Commerce
Subcommittee on Oversight and Investigations
"Security of HealthCare.gov"
November 19, 2013

Good morning, Chairman Murphy, Ranking Member DeGette, and members of the Subcommittee. Since the passage of the Affordable Care Act, the Centers for Medicare & Medicaid Services (CMS), in partnership with private sector contractors, has been hard at work to design, build, and test secure systems that ensure Americans are able to enroll in affordable health care coverage. I serve as CMS's Deputy Chief Information Officer (CIO), and I am a career civil servant. As Deputy CIO, my role has been to guide the technical aspects of Marketplace development and implementation in accordance with all applicable laws, regulations, and agreements. While consumers using HealthCare.gov have been frustrated in these initial weeks after the site's October 1, 2013 launch, CMS is working around the clock to address problems so that the site works smoothly for the vast majority of users by the end of this month.

Overview of Marketplace Information Technology (IT)

The Affordable Care Act directs states to establish State-based Marketplaces by January 1, 2014. In states electing not to establish and operate such a Marketplace, the Affordable Care Act requires the Federal Government to establish and operate a Marketplace in the state, referred to as a Federally-facilitated Marketplace. The Marketplace provides consumers access to health care coverage through private, qualified health plans, and consumers seeking financial assistance may qualify for insurance affordability programs like Medicaid, the Children's Health Insurance Program (CHIP), or the advance payment of the premium tax credits and cost-sharing reductions that can lower consumers' upfront and out-of-pocket costs.

Marketplace IT System Functions

To fulfill the functions specified in the Affordable Care Act, Federally-facilitated and State-based Marketplaces developed eligibility and enrollment, redetermination, and appeals systems. In many ways, these systems are similar to what private issuers, Medicare Advantage issuers,

and State Medicaid agencies currently use to determine eligibility, enroll applicants into health coverage, process appeals, and perform customer service, as well as prevent fraud, waste, and abuse.

These systems:

- Determine a consumer's eligibility to enroll in a qualified health plan through the Marketplace and for insurance affordability programs;
- Transmit consumer information to state Medicaid/CHIP agencies or the private, qualified health plan issuer they have chosen;
- Redetermine consumer eligibility status during the year, as needed; and
- Allow individuals to appeal an eligibility determination.

Privacy, Security, and Integrity Controls for the Marketplace IT Systems

A key feature of the Marketplace IT systems is that they employ stringent privacy and security controls to safeguard consumer data. CMS developed the data services Hub and Federally-facilitated Marketplace eligibility and enrollment system consistent with Federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS' IT systems—including Federal Marketplace systems of records and systems used to support State-based Marketplaces and Medicaid/CHIP agencies—are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002 (FISMA). These systems must also comply with various rules, regulations, and standards promulgated by the Department of Health and Human Services (HHS), the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology (NIST).

Key Marketplace IT Functions

To facilitate the back-end online eligibility and enrollment, redetermination, and appeals functions consumers access through HealthCare.gov, CMS developed two key tools, in partnership with private sector contractors. CMS contracted with QSSI to build the Hub, which provides an electronic connection between the eligibility systems of the Marketplace and State Medicaid and CHIP agencies to already existing, secure Federal and state databases to verify the information consumers provide in their applications for coverage. In addition, CMS contracted

with CGI Federal to build the Federally-facilitated Marketplace eligibility and enrollment system, which consumers use to create an account on HealthCare.gov, verify their identity, fill out an electronic application to determine their eligibility for health care coverage through private, qualified health plans, Medicaid, CHIP or other insurance affordability programs, choose a health insurance plan and ultimately enroll in health coverage.

The Data Services Hub

CMS designed the Hub, a routing tool that helps the Marketplace and State Medicaid and CHIP agencies provide accurate and timely eligibility determinations. The Hub verifies data against information contained in already existing, secure and trusted Federal databases. CMS has security and privacy agreements with all Federal agencies and states connecting to the Hub. These include the Social Security Administration, the Internal Revenue Service, the Department of Homeland Security, the Department of Veterans Affairs, Medicare, TRICARE, the Peace Corps and the Office of Personnel Management. The Hub increases efficiency and security by eliminating the need for each Marketplace, Medicaid agency, and CHIP agency to set up separate data connections to each database. Risk increases when the number of connections to a data source increase—which is why CMS has designed the Hub to minimize these risks. The Hub provides one highly secured connection among trusted Federal and state databases instead of requiring each agency to set up what could have amounted to hundreds of independently established connections. Further, the Hub is not a database; it does not retain or store information. It is a routing tool that can validate applicant information from various trusted Government databases through secure networks.

Every Federal IT system must comply with rigorous standards before the system is allowed to operate. The Hub's independent Security Controls Assessment was completed on August 23, 2013 and it received an authorization to operate on September 6, 2013. This authorization confirms that the Hub complies with Federal standards and that CMS implemented the appropriate procedures and safeguards necessary for the Hub to operate securely.

The Hub and the Federally-facilitated Marketplace eligibility and enrollment system have several layers of protection in place to mitigate information security risk. For example, these

Marketplace IT systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action against irregular behavior and unauthorized system changes that could indicate a potential incident. If a security incident occurs, an Incident Response capability would be activated, which allows for the tracking, investigation, and reporting of incidents. This allows CMS to quickly identify security incidents and ensure that the relevant law enforcement authorities, such as the HHS Office of Inspector General Cyber Crimes Unit, are notified for purposes of possible criminal investigation. As with all systems, the responsibility to safeguard information is an ongoing process, and CMS will remain vigilant throughout operations to anticipate and protect against data security concerns. The Marketplace IT monitoring program will continually be reviewed for effectiveness of the IT's security controls, through methods that include independent penetration testing, automated vulnerability scans, system configuration monitoring, and active web application scanning.

The Federally-Facilitated Marketplace Eligibility and Enrollment System

As described above, the Affordable Care Act directs states to establish State-based Marketplaces by January 1, 2014. In states electing not to establish and operate such a Marketplace, the Affordable Care Act requires the Federal Government to establish and operate a Marketplace for the state, referred to as a Federally-facilitated Marketplace. CMS contracted with CGI Federal to build the Federally-facilitated Marketplace system, including the eligibility and enrollment system. This system lets consumers establish a HealthCare.gov account that they can return to at any point in the application process, and the system connects to the Hub to validate the information consumers submit. Once consumer information is verified, the eligibility and enrollment system forwards consumer applications to an eligibility tool to determine the consumer's eligibility for Medicaid, CHIP, or tax subsidies. For those consumers eligible for tax subsidies, it then allows consumers to compare qualified health plans and start to enroll in the plan of their choosing, transferring the consumer's information to the issuer to complete the enrollment process.

Separate from the Federally-facilitated Marketplace eligibility and enrollment system on HealthCare.gov is a premium estimation tool, launched on October 10, 2013, that allows consumers to browse health plans without creating a HealthCare.gov account. While the tool

could only sort consumers into two age categories when it was first launched, its functionality will be expanded to accommodate additional scenarios to better fit consumer shopping profiles. This tool is different from the Federally-facilitated Marketplace application because determinations about consumers' eligibility for insurance affordability programs, Medicaid, and CHIP are specific to the characteristics of an applicant and his or her household and can only be calculated when an application is completed—after income, citizenship, and other information is verified.

The Federally-facilitated Marketplace eligibility and enrollment system consists of numerous modules. Each module of this system was tested for functionality. Each interface with our business partners and other Federal agencies was also tested. Numerous test cases were used to exercise the end-to-end functionality of the system. Given the user experience, we know now that we underestimated the volume of users who would attempt to log onto the system at the same time, and therefore our testing did not include performance testing at the volume we experienced at launch.

On September 27, 2013, CMS granted authority for the Federally-facilitated Marketplace eligibility and enrollment system to begin operations, with authority to operate for six months. Consistent with security practices as required by FISMA and NIST, CMS identified a number of strategies that we are deploying to continue to monitor operations and mitigate any potential risk, including through regular additional testing. The authorization to operate the Federally-facilitated Marketplace eligibility and enrollment system is consistent with NIST guidance. FISMA and the NIST Risk Management framework permit agencies to authorize an "authority to operate" when there is a risk-mitigation strategy in place. To follow through on the risk mitigation strategy identified in the authorization to operate the Federally-facilitated Marketplace eligibility and enrollment system, we continue to conduct security testing on an ongoing basis as we add new IT functionality.

Improvements to the Federally-facilitated Marketplace Eligibility and Enrollment System

While the Hub is working as intended, after the launch of the Federally-facilitated Marketplace eligibility and enrollment system, numerous unanticipated technical problems surfaced which

have prevented some consumers from moving through the account creation, application, eligibility, and enrollment processes in a smooth, seamless manner. Some of those problems have been resolved, and the site is functioning much better than it did initially. We are committed to fixing these problems so that the experience using the Federally-facilitated eligibility and enrollment system improves for the vast majority of consumers by the end of November 2013.

To ensure that we make swift progress, and that the consumer experience continues to improve, our team called in additional help to solve some of the more complex technical issues we are encountering. We brought on board management expert and former CEO and Chairman of two publicly-traded companies, Jeff Zients, to work in close cooperation with our team to provide management advice and counsel to the project. We have also enlisted the help of QSSI to serve as a general contractor for the project. They are familiar with the complexity of the system, and the work they provided—the Hub—is working well and performing as it should. They are working with CMS leadership and contractors to prioritize the needed fixes and make sure they get done.

A number of fixes have already been completed. One place where we have seen a lot of consumer frustration is in the ability to successfully create an account. This issue is something that we identified on October 1, and we have made significant progress since then to deliver a much smoother process for consumers. Users can now successfully create an account and continue through the full application and enrollment process. We are now able to process nearly 17,000 registrants per hour, or 5 per second, with almost no errors.

The tech team put into place enhanced monitoring tools for HealthCare.gov, enabling us to get a high level picture of the Federally-facilitated Marketplace eligibility and enrollment system. Thanks to this work, we are now better able to see how quickly pages are responding, and to measure how changes improve user experience on the site.

We reconfigured various system components to improve site responsiveness. This has increased performance across the site, but in particular the viewing and filtering of health plans during the

online shopping process now responds in just seconds. It was taking minutes. We have also resolved issues with how the eligibility notices are presented to consumers. They now display properly at the completion of the application process.

Other fixes include software configuration changes and optimization that have increased the efficiency of system interactions. We also added capacity by doubling the number of servers and have replaced the virtual database with a high-capacity physical one. This allowed us to be more efficient and effective in our processing time and significantly reduced the account registration failures. While significant work remains, these changes are already making the shopping process easier for consumers.

Conclusion

CMS is committed to creating safe, secure, and resilient IT systems that help expand access to the quality, affordable health coverage every American needs. We are encouraged that the Hub is working as intended, and that the framework for a better-functioning Federally-facilitated Marketplace eligibility and enrollment system is in place. By enlisting additional technical help, aggressively monitoring for errors, testing to prevent new issues from cropping up, and regularly deploying fixes to the site, we have already made significant improvements to the performance and functionality of the system. We expect that over the next few weeks, consumers will see improvements to the site each week, and that the consumer experience using the Federally-facilitated Marketplaces eligibility and enrollment system through HealthCare.gov will be greatly improved for the vast majority of users by November 30.

Mr. MURPHY. Thank you, Mr. Chao. I will recognize myself first for 5 minutes.

Mr. Chao, for the last year, members of this committee have asked you and others in the administration about the status of the launch of the President's healthcare law. We wanted to know if you would be ready for the October 1 start of enrollment. Over and over, we were assured that all was well and everything was on track.

The documents produced to the committee show a different picture, and I would like to walk through a couple of them with you.

In mid-March, you made a candid comment that you didn't want the Exchange Web site to be a Third World experience. Now the committee has learned about a report prepared by committee for senior HHS and White House officials, and presented to these officials in late March and early April this year. That document is tab 1 of your document binder. This document highlights a number of risks facing Healthcare.gov's launch, late policy, delayed designs, and building time and limited to a test.

When did you first see this presentation?

Mr. CHAO. I haven't seen that presentation.

Mr. MURPHY. You were not briefed at all that there was a McKinsey report presentation going on?

Mr. CHAO. I knew that McKinsey had been brought in to conduct some interviews and assessments and report to our administrator, in which I actually participated in some of those——

Mr. MURPHY. You participated in the interviews when McKinsey was exploring this?

Mr. CHAO. Right, but I was not given the final report.

Mr. MURPHY. Were you aware that they had met with Secretary Sebelius, Marilyn Tavenner, Gary Cohen and others at CMS Headquarters, HHS Headquarters, the Executive Office Building and the White House?

Mr. CHAO. We——

Mr. MURPHY. Any of those incidences?

Mr. CHAO. I believe there were some meetings that I heard of, but I don't know the exact dates when they occurred.

Mr. MURPHY. Now, part of your job is to make sure that this Web site is working, am I correct?

Mr. CHAO. Correct.

Mr. MURPHY. And so this was a major report that went as high up as the Secretary, maybe others, we don't know, but saying that there were serious problems with this. And you are saying that, even though you were interviewed by this, you did not ever have this briefing yourself?

Mr. CHAO. No, I didn't.

Mr. MURPHY. You knew it existed?

Mr. CHAO. I had heard that there was a final report out, but I didn't see the actual report.

Mr. MURPHY. Did anything change for you in recognizing that this report was out there, basically telling people working on the HHS Web site that there were serious problems, no end-to-end testing, that other various aspects of it?

Mr. CHAO. I can't really tell you or speak to you of the contents of that report because I did not see it, and I didn't hear about it until actually it was in The Washington Post.

Mr. MURPHY. I mean certainly, this is part of the concerns we have, and we are not making this stuff up. It is a matter that we have a Web site out there which untold millions, tens of millions or hundreds of millions are spent on this Web Site, which you have major leadership role here. McKinsey is hired to come and present what the problems are, and lay out a roadmap of those problems. I am deeply concerned that this is something that you knew existed but had not read.

So when were you first concerned that the administration wasn't going to be ready October 1 for the start of the open enrollment?

Mr. CHAO. I never thought that. I had relative——

Mr. MURPHY. But you made a comment about you didn't want this to be a plane crash.

Mr. CHAO. Well, you are referring to the email——

Mr. MURPHY. Yes.

Mr. CHAO [continuing]. Exchange that I had with several——

Mr. MURPHY. Yes, certainly that email didn't say everything is going fine, congratulations team.

Mr. CHAO. Of course—I——

Mr. MURPHY. It said I don't want this to be a—so you must have had some awareness that some problems existed.

Mr. CHAO. Chairman, you have to understand, and the committee, that I have been working on this since mid-2010——

Mr. MURPHY. And we appreciate that.

Mr. CHAO [continuing]. And I have—I am a very cautious and—you know, I err on the side of caution and urgency because, even back in 2010, I didn't believe that, you know, everything would be easy and just, you know, going along smoothly. So on a regular basis, I work with a lot of my contractors and my staff to sensitize them on the sense and level of urgency that is involved.

Mr. MURPHY. Absolutely. Especially with McKinsey was called in to prepare this document which was important enough for them to have meetings at CMS, HHS, with the Secretary of Health and Human Services, at the Executive Office Building and at the White House, describing the level of problems. So I appreciate your sensitivity and awareness to that. I am concerned you saying you have not even read this yet.

Your testimony mentions the use of sensors and active event monitoring. You state that if an event occurs, an instant response capability is activated. Has that happened yet?

Mr. CHAO. Yes.

Mr. MURPHY. How many times?

Mr. CHAO. You mean whether if we are conducting——

Mr. MURPHY. No, an instant response——

Mr. CHAO [continuing]. An instant response——

Mr. MURPHY [continuing]. Capability. Well, first of all, has anything happened yet, any hackers, any breaches, anyone trying to get into the system from the outside, has that occurred yet?

Mr. CHAO. I think that there was 1 incident that I am aware of, but it requires that we go to a classified facility and to actually——

Mr. MURPHY. Only once since the—where—but you are saying no other attempts to breach into this system have occurred?

Mr. CHAO. Not successful ones, no.

Mr. MURPHY. Not since when?

Mr. CHAO. Not successful ones.

Mr. MURPHY. All right. Now, when there are attempts, who do you report this to?

Mr. CHAO. It is a combination of a series of authorities that are involved.

Mr. MURPHY. Law enforcement?

Mr. CHAO. Well, through our incident reporting and breach reporting processes that go through our agencies, various key leadership and then up through the department, as well as we have a Security Incident Response Center at the department that works with US–CERT at DHS.

Mr. MURPHY. Thank you. We will follow-up subsequently.

I know I am out of time, so we will now recognize Ms. DeGette for 5 minutes.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

First of all, Mr. Chao, and also to the contractors, something you said in your opening I think we should really take heed, which is you want to be careful not to divulge sensitive information about the security designs of the Web site. Is that right?

Mr. CHAO. That is correct.

Ms. DEGETTE. So I would say to you and to the contractors, and I think the majority would agree with me, if there is a question asked about that sensitive information, if you would just let us know and then we can take it into executive session, or whatever we need to do.

Ms. MURPHY. Absolutely.

Mr. CHAO. Certainly.

Ms. DEGETTE. Thank you, Mr. Chairman.

Now, Mr. Chao, the chairman was asking you about this memo that you had—or it is an email, and it was on Tuesday, July 16. If you can take a look at tab 7 in your document binder, please. That is a copy of your memo, and it looks to me in reading it that you were basically telling people that you wanted to make sure this Web site got up and going. Is that right?

Mr. CHAO. Yes.

Ms. DEGETTE. And that was your view, right?

Mr. CHAO. Yes.

Ms. DEGETTE. Did you take further actions after July 16 to try to get the Web site up and going?

Mr. CHAO. It was a constant daily effort.

Ms. DEGETTE. And it still is, isn't it?

Mr. CHAO. To improve it, certainly.

Ms. DEGETTE. Yes. OK, I would like you now to take a look at tab 1 of your document binder. Now, Mr. Chao, this is the document that was given to The Washington Post yesterday by the majority, and also simultaneously to the Democrats on the committee. This is the document the chairman was asking you about in his opening statement. Have you ever seen this document before?

Mr. CHAO. No, I haven't.

Ms. DEGETTE. OK, so you don't really know about whatever it might have said in that document, right?

Mr. CHAO. No, I——

Ms. DEGETTE. OK, thanks.

Mr. CHAO. I believe it is an executive level briefing for——

Ms. DEGETTE. Right, but you weren't—you didn't—you weren't part of that briefing?

Mr. CHAO. No.

Ms. DEGETTE. OK. That doesn't mean though that you weren't concerned about the Web site working and trying to make it work.

Mr. CHAO. Well, of course. I think in some of the interviews with McKinsey, you know, I think some of what is in here could have potentially come from information that——

Ms. DEGETTE. But you wouldn't know that because you didn't see it.

Mr. CHAO. No, I——

Ms. DEGETTE. OK.

Mr. CHAO [continuing]. Don't see how it was formed.

Ms. DEGETTE. I want to talk to you about the topic of this hearing now for a few minutes, and that is the issue of security. And I think I heard you say both in your opening and in response to questioning by the chairman, I just wanted to ask again. Have there been vulnerabilities that have been discovered since the Web site unveiled on October 1?

Mr. CHAO. Security vulnerabilities——

Ms. DEGETTE. Yes.

Mr. CHAO [continuing]. Have not necessarily been reported in terms of it being a security threat. I think there was some misuse of terminology of something like 16 incidents reported that—in a previous DHS testimony a couple of days ago, but they were actually incidents involving disclosure of PII information, and it wasn't due to the result of anyone trying to attack the Web site.

Ms. DEGETTE. What was it a result of?

Mr. CHAO. It was dealing with some training issues at the call center, or we had a system issue where if you had similar usernames and you chose a special character at the end of that username, for example, if your name is Smith and you chose an @ sign at the end of the username, sometimes that @ sign was treated like a—what we call a wildcard search, so the return log-in information about someone else, but that since—since was reported, has been fixed as of today.

Ms. DEGETTE. That problem has been fixed so that is——

Mr. CHAO. Yes.

Ms. DEGETTE [continuing]. Not happening anymore?

Mr. CHAO. It is not a hacker——

Ms. DEGETTE. Now, you have been at the Agency how long, sir?

Mr. CHAO. Approximately 20 years.

Ms. DEGETTE. And in working on the other sensitive areas, Medicare and other areas, is this common that sometimes there might be a little bump like this?

Mr. CHAO. Fairly common.

Ms. DEGETTE. Uh-huh, and what does the Agency do when that is identified?

Mr. CHAO. We have an extensive set of processes and controls in place with designated personnel to handle whether they are——

Ms. DEGETTE. And——

Mr. CHAO [continuing]. For example, security breaches versus the personally identifiable information-type incidents, data loss.

Ms. DEGETTE. And there is continuing testing, is that right?

Mr. CHAO. Correct.

Ms. DEGETTE. Now, MITRE has been performing assessments for CMS, is that correct?

Mr. CHAO. Correct.

Ms. DEGETTE. And what that does is it gives the contractors the opportunity to identify and resolve security vulnerabilities, is that correct?

Mr. CHAO. I think what is—the benefit is that we use a set of contractors to independently test the system so that we are not taking the words of, let us say, for example, QSSI or CGI themselves performing security testing. So this independent testing provides us a more, you know, balanced view of——

Ms. DEGETTE. And is this ongoing, this——

Mr. CHAO. Yes.

Ms. DEGETTE [continuing]. This independent testing?

Mr. CHAO. It is on a daily and weekly basis.

Ms. DEGETTE. Thank you very much, Mr. Chairman.

Mr. MURPHY. The Chair now recognizes Mr. Barton for 5 minutes.

Mr. BARTON. Thank you, Mr. Chairman.

In Mr. Dingell's opening statement, and to some extent what Ms. DeGette just said, I am reminded of the movie "Casablanca," and Claude Rains, the French chief of police, goes into Rick's Café and says, "I am shutting it down, I am shutting it down." And Rick comes up, who is played by Humphrey Bogart, and says, "Why are you shutting us down?" And Claude Rains, the chief of police, says, "I am shocked, shocked, to learn there is gambling going on," just as the croupier comes up and says to Claude Rains, "Your winnings, sir."

It is interesting and amusing that the past master running this committee, Mr. Dingell, would be shocked, shocked and amazed that something was given to The Washington Post yesterday. Now, I am not saying that it was, I don't know, but if it did happen, it wouldn't be the first time in this committee's history that documents were given to the press at approximately the same time they were distributed to the members of the committee.

Mr. DINGELL. If the gentleman would yield, I didn't say I was shocked, I said I was grateful I had the subscription to The Washington Post so I could keep track of what——

Mr. BARTON. Well——

Mr. DINGELL [continuing]. Is going on in the committee——

Mr. BARTON. Well——

Mr. DINGELL [continuing]. Along with my Republican——

Mr. BARTON [continuing]. Reclaiming my time from my—which is my time, from my good friend. What shocks me is that Mr. Chao, our witness, who is the Deputy Chief Information Officer and Deputy Director of the Office of Information and Services for Medicare and Medicaid, who has been identified numerous times as the chief

person in charge of preparing this Web site at the CMS level, was not aware of this document. I mean to me, that is what is shocking.

So my first question to you, sir, is when were you made aware of this McKinsey briefing document?

Mr. CHAO. I think I was aware that some document was being prepared, because I had gone through the interviews, but towards the end when the briefings occurred, I was not part of them, nor was I given a copy.

Mr. BARTON. I mean, were you aware that McKinsey had been hired to come in and basically troubleshoot the status of the Web site?

Mr. CHAO. I don't think they were brought in to troubleshoot, I think they were brought in to make an assessment by conducting various interviews with key——

Mr. BARTON. Did——

Mr. CHAO [continuing]. Stakeholders.

Mr. BARTON. Did this group ever talk to you?

Mr. CHAO. Yes.

Mr. BARTON. OK, so they did come in and at least visit with you?

Mr. CHAO. Yes, they have interviewed me before.

Mr. BARTON. Once, twice, a dozen?

Mr. CHAO. Probably at least two times from what I recall.

Mr. BARTON. OK. Now, since you have been made aware of the document——

Mr. CHAO. Well, I——

Mr. BARTON [continuing]. Have you studied it?

Mr. CHAO. No, I was not made aware of the document. I was interviewed by the team that put that together. When the document was assembled, I didn't get a copy of it.

Mr. BARTON. OK. Well, as Mr. Dingell has pointed out, it is in The Washington Post. So have you—before coming before this subcommittee this morning, have you perused this document?

Mr. CHAO. No, I have not.

Mr. BARTON. You have not perused this document, OK. Well, on page 1 of the document, it says the working group, whoever that is, maybe you can enlighten us on that, determined that extending the go-live date, which, as we all know, is October the 1st, should not be a part of the analysis and, therefore, worked with a boundary condition of October the 1st as the launch date. Now, in plain English, what that means is somebody decided we couldn't delay the startup date so, by golly, we are going to assume it is going to go live on October the 1st.

Were you a part of the working group that made that decision?

Mr. CHAO. No.

Mr. BARTON. Do you know who the working group was that made that decision?

Mr. CHAO. No.

Mr. BARTON. Do you have any idea, was it the President and the Secretary of Health and Human Services, or was it somebody below your level that made a decision somewhere in the bowels of the bureaucracy?

Mr. CHAO. I think that it probably was a conglomerate of several——

Mr. BARTON. A conglomerate?

Mr. CHAO [continuing]. Key leadership that came to that conclusion.

Mr. BARTON. OK. Did you——

Mr. CHAO. I was——

Mr. BARTON. Did you have any decision-making authority yourself about when the start-up date should be?

Mr. CHAO. No.

Mr. BARTON. That was not in your authority to say we are going to have to put it off or make a decision to go forward?

Mr. CHAO. No, I do not get to pick what date.

Mr. BARTON. Do you know who did have that decision-making authority?

Mr. CHAO. I believe it is our administrator, Marilyn Tavenner, and potentially other folks, but primarily I take my direction from Marilyn Tavenner.

Mr. BARTON. All right. Well, Mr. Chairman, my time has expired, but I will just say in summing up, we are concerned at multiple levels, but if you review this CMS document, which I did not see until just now, this morning, it doesn't take but about 10 minutes to go through and look at it, and it is absolutely clear that the startup of the Web site was not going to work well, if at all, on October the 1st. It was not. And it says that in here.

So with that, I yield back.

Mr. MURPHY. Thank you. Gentleman's time has expired.

The Chair now recognizes Mr. Dingell for 5 minutes.

Mr. DINGELL. Chairman, I thank you for the recognition and thank you for holding this hearing.

We are over 6 weeks into the implementation of the Affordable Care Act, and while the functionality of the Healthcare.gov Web site has improved, it is clear there is more work to be done, and I am hopeful that the subcommittee will work hard to achieve that goal.

ACA is the law of the land, and I believe we share the goal of making it a functioning and secure Web site, however, it is important to remember that we can never fully eliminate the risks when building a large IT system, and so we must take steps to mitigate them. I would also urge that we take the necessary steps to make the program work, because this is the largest undertaking of this character I believe that we have ever seen by a Government anywhere.

First question, yes or no. Is CMS responsible for developing the Data Services Hub and the eligibility enrollment tools for the Federally Facilitated Marketplace? Yes or no, Mr. Chao?

Mr. CHAO. Yes.

Mr. DINGELL. Now, Mr. Chao, are these projects required to comply with the Privacy Act of 1974, the Computer Security Act of 1987, the Federal Information Security Management Act of 2002? Yes or no?

Mr. CHAO. Yes.

Mr. DINGELL. Now, additionally, CMS must also comply with regulations and standards promulgated by the National Institute of Standards and Technology at the U.S. Department of Commerce. Is that correct?

Mr. CHAO. Yes.

Mr. DINGELL. Now, these NIST standards require CMS to balance security considerations with operational requirements. Is that correct?

Mr. CHAO. Yes.

Mr. DINGELL. Mr. Chao, once the key pieces of Healthcare.gov Web site is the Data Hub. Is this a large repository of personal information as some of my friends on the other side have claimed? Yes or no?

Mr. CHAO. No.

Mr. DINGELL. Say that again. No?

Mr. CHAO. No, it does not store any——

Mr. DINGELL. OK, I want——

Mr. CHAO [continuing]. Personal——

Mr. DINGELL. I want that on the record and clearly heard. Does the Data Hub retain any personal information at all? Yes or no?

Mr. CHAO. No.

Mr. DINGELL. Indeed, is it fair to say that the Data Hub is a tool to transmit eligibility information to Federal agencies? Yes or no?

Mr. CHAO. Yes.

Mr. DINGELL. Now, did the Data Hub pass a security test to the October 1 launch of Healthcare.gov? Yes or no?

Mr. CHAO. Yes.

Mr. DINGELL. All right, is the Data Hub working as intended today? Yes——

Mr. CHAO. Yes.

Mr. DINGELL [continuing]. Or no?

Mr. CHAO. Yes.

Mr. DINGELL. And is there any evidence to the contrary?

Mr. CHAO. No.

Mr. DINGELL. Is there any evidence of breaches or lack of security of personal data or information by any person who has submitted such data to this undertaking? Yes or no?

Mr. CHAO. No.

Mr. DINGELL. It is always true—our duty to remember how our healthcare system operated prior to the passage of the ACA. At that time, insurance companies were allowed to medically underwrite people to determine their premium. This required lengthy, confusing applications, and contained a lot of personal medical information. Oftentimes this was submitted electronically as well. ACA has changed all of this.

Now, in fact, this is a question to you again, Mr. Chao. In fact, application forms on Healthcare.gov do not require the submission of any personal health information. Is that correct, yes or no?

Mr. CHAO. Yes.

Mr. DINGELL. Now, Mr. Chao, that is because ACA prohibits discrimination on the basis of pre-existing conditions, and outlaws charging people more because they are sick. Is that correct?

Mr. CHAO. Yes.

Mr. DINGELL. So the information is not necessary?

Mr. CHAO. It is not.

Mr. DINGELL. And it is not correct—and it is not collected?

Mr. CHAO. It is not collected.

Mr. DINGELL. All right, this is a remarkable improvement over the old system in terms of both security and the quality of care.

Next question. There are a lot of negative stories in the press that create a lot of confusion, so I want to get this record straight.

Is Healthcare.gov safe and secure for my constituents to use today with regard to protection of their personal information and their privacy? Yes or no?

Mr. CHAO. Yes.

Mr. DINGELL. Is there any evidence at all to the contrary?

Mr. CHAO. No.

Mr. DINGELL. Mr. Chairman, you have been most gracious. I yield you back 12 seconds.

Mr. MURPHY. Thank you.

Now going to recognize Mrs. Blackburn for 5 minutes. Thank you.

Mrs. BLACKBURN. Thank you, Mr. Chairman.

Mr. Chao, we really appreciate that you would come and work with us on this issue. I want to talk with you for a minute about some red flags that seemed to be apparent to you, and you are going to find the email I am referencing at tab 7, and it is the July 16, 2013, email that you sent to Monique Outerbridge. And I really want to focus there. You know, when you have something that is running off the rails and—as this obviously seemed to you to be doing, it was a project that just was not proceeding as it should be proceeding, and you expressed these concerns about the performance of CGI, what I would like to hear from you is just an articulation of maybe what were those top 3 or 4 red flags that seemed to be going up to you, that you said I fear that the plane is going to crash on takeoff, and some of those wordings that we have heard from you now.

So give me just kind of the top 3 or 4 things.

Mr. CHAO. I think in the context of this email, it was at a time period in which we were getting ready to roll out what we called Light Account, which is that initial registration process. And as I mentioned before, I am a person who has a lot of anxiety and I always err on the side of caution if we are going to run out of time, so I occasionally get a little passionate in my emails to remind people that they need to move fast, and if they are moving fast, they need to move faster. That is just the way I operate and the way I direct staff and contractors. And what I was afraid of was, at this particular point in time, was that we were falling behind in the rollout of Light Account.

Mrs. BLACKBURN. OK, on Light Account, did your test on that go off without a hitch, or what happened?

Mr. CHAO. There—I don't exactly remember the specifics about what tests passed or failed, I just was afraid that we were in jeopardy of missing the date. So, therefore, you know, I—at that time period, starting July, I wrote lots of emails to try to——

Mrs. BLACKBURN. OK, did you hit the date?

Mr. CHAO. I believe we—it took an extra 4 days.

Mrs. BLACKBURN. An extra 4 days?

Mr. CHAO. Yes.

Mrs. BLACKBURN. On the test. And you don't remember exactly what the concerns were that came to you at that point in time. Is there a memo of review, a memo, an articulation of what——

Mr. CHAO. I——

Mrs. BLACKBURN [continuing]. Transpired in that test process?

Mr. CHAO. I don't think it is necessarily a memo. I think the way we operate is that we have daily meetings and——

Mrs. BLACKBURN. Are there minutes from those meetings——

Mr. CHAO [continuing]. We——

Mrs. BLACKBURN [continuing]. And could you submit those to us for the record?

Mr. CHAO. I don't believe that there were minutes. I believe they were just status check-ins with, you know, contractors and their——

Mrs. BLACKBURN. Are there notes?

Mr. CHAO. No, I don't——

Mrs. BLACKBURN. Informal notes?

Mr. CHAO. I don't believe so. I think when my emails were——

Mrs. BLACKBURN. OK.

Mr. CHAO [continuing]. Submitted as evidence——

Mrs. BLACKBURN. OK.

Mr. CHAO [continuing]. That is kind of a——

Mrs. BLACKBURN. All right, let me go on a minute. I want to talk specifically about CGI. What about, you know, if you all kind of informally worked in a group, and didn't have formal meetings or minutes and memos and things of that nature, just give me your impression, what was it—your perception that caused you to lose confidence in CGI, where were you on that, because I think it is so interesting, you mentioned price and I note in this email chain from Monique Outerbridge that they had $40 million already that they had taken, they were coming back and asking for another $38 million. Now, if I had someone who had used up all of their money from a project, and then they came back and asked for that much more, I think I would have to say, wait a minute. So regardless, obviously, the price to you was of tremendous concern. Am I right on that?

Mr. CHAO. Correct.

Mrs. BLACKBURN. OK, so they had already kind of washed your confidence there. What else was it in their conduct that eroded your confidence in their ability to transact this portion of business?

Mr. CHAO. I think what I was trying to say is that, relatively speaking to, I would say, most project managers that are looking at smaller-scale projects, I would say there might be some room to be——

Mrs. BLACKBURN. OK——

Mr. CHAO [continuing]. A little more confident, but given the task at hand, my confidence level had to deal with the enormous amount of activities we had to be successful at to deliver, you know, on Light Account, that interim, you know, kind of piece, as well as the October 1 delivery.

Mrs. BLACKBURN. I yield back.

Mr. MURPHY. Yes, I am just curious, to follow-up to that. Did you ever present these concerns that you had about being ready—whether or not it would be ready on October 1, when you were interviewed by McKinsey people?

Mr. CHAO. Well, this was in the July time frame. I think McKinsey was—their interviews were in maybe a March or April time frame.

Mr. MURPHY. I just wondered if you presented any concerns to them about being able to meet these dates when you spoke with them?

Mr. CHAO. I think as a course of conducting project management, program management, that working with CGI and QSSI and my team, we discussed these concerns on an ongoing basis. In——

Mr. MURPHY. Just one note. I will follow up——

Mr. CHAO. OK.

Mr. MURPHY. We will make sure someone follows up.

Now I will recognize Mr. Waxman for 5 minutes.

Mr. WAXMAN. And thank you, Mr. Chairman.

Nobody is happy with this rollout of Healthcare.gov, and the administration has taken its lumps, but aside from lessons learned, it seems to me that my focus ought to be and my concern is getting this thing working. Americans want to be able to access the Web site and choose a healthcare plan, especially those who haven't been able to get an opportunity to buy health insurance in the past. That is why it seems to me, if we need legislative changes, we should make changes to make it work, not to repeal it. You know, the Republicans are so fixated on hating this law and they want to repeal it. They don't even want to consider helping make it work, and that is the focus that I want to use in asking you some questions, Mr. Chao. How do we make this work better?

Now, is it accurate to say that CMS is getting the Web site up and running?

Mr. CHAO. Yes.

Mr. WAXMAN. OK, and is it accurate that CMS has crossed—Center for Medicare and Medicaid Services, that is the department—part of HHS that is working on it, they have crossed 200 items off its punch list?

Mr. CHAO. Correct.

Mr. WAXMAN. And can you give me a few examples of important issues that have recently been addressed?

Mr. CHAO. Issues related to the enrollment transactions that had some data issues—data quality issues that were fixed, and now issuers can receive that data without doing a lot of cleaning up of that data. So——

Mr. WAXMAN. Um-hum.

Mr. CHAO [continuing]. Data quality has improved. The daily transactions that we send to them have improved.

Mr. WAXMAN. Um-hum.

Mr. CHAO. The response times for the Web site have improved. The error rate of people experiencing some level of difficulty with moving from stage to stage in their online application, that has been reduced and improved.

Mr. WAXMAN. Well, in fact, Jeff Zients, the administration's point person on this whole Web site, announced on Friday that you have dropped your error rate from 6 percent to below 1 percent, and you have cut the average wait time for page loading from 8 seconds to less than 1 second. What do these improvements look like to the average consumer going on the site?

Mr. CHAO. I think they become transparent to the user. The user then can get at the task at hand of filling out their information, of finding out if they are asking for a premium tax credit, that they

are calculated timely, and they are proceeding ahead in the application so that they can apply some, all or none of that premium tax credit to their plan compare so that they can look at the offsets that occur, and what the final premium should be, to make their selection and to go through the process in a very efficient and speedy fashion, as compared to what they experienced on day 1.

Mr. WAXMAN. How about the overall stability of the site? It was down frequently in the early weeks. Has that improved?

Mr. CHAO. Yes, certainly. I think we do have regular maintenance windows, but those maintenance windows are used to implement these improvements that you have been hearing about.

Mr. WAXMAN. So numbers seem to be getting better, and I expect we will see more improvements. The anecdotal evidence I get is that the site is getting better, slowly but surely, and that explains why the enrollment rate in November is speeding up significantly. In fact, I do have more than anecdotes, I have some figures. In Massachusetts, where they started a similar program, it started off slowly, only 3/10 of a percent of overall enrollees for private coverage signed up in the first month, and then thus far, in the Affordable Care Act, 1.5 percent. So both started slowly. We are even ahead of what Massachusetts was. But after that, there was a surge in enrollment as people got closer to deadlines.

The LA Times reported that "a number of States that use their own systems are on track to hit enrollment targets for 2014 because of a sharp increase in November." California, which enrolled 31,000 people in private plans last month, nearly doubled that in the first 2 weeks of this month, and several other States are outpacing their enrollment estimates. In Minnesota, enrollment in the second half of October was triple the rate of the first half. So we see an acceleration, even in the Federal Marketplace. The New York Times reported that the Federal Marketplace has nearly doubled its private plan enrollment in just the first 2 weeks of November.

We are not where we need to be, but we are seeing improvements, and this increased pace of people going back on the site successfully is, to me, very encouraging. So rather than just attack the healthcare law or look for ways to undermine it, we ought to try to make it work, and we are anxious to make sure that you do your job of getting the Web site and all of that working, and if we need any legislative change, call on us because we are ready, willing and able to act in that regard.

Yield back my time.

Mr. MURPHY. The gentleman's time has expired.

I now recognize for 5 minutes the gentleman from Texas, Dr. Burgess.

Mr. BURGESS. And thank you, Mr. Chairman. Thank you again, Mr. Chao, for being here.

In response to one of Dr. Murphy's questions about a breach of the system, you responded that you could not talk about it in open session, that it would require a classified briefing. Is that correct? Did I hear you correctly?

Mr. CHAO. Correct. That was—that is how I was instructed by our department.

Mr. BURGESS. Very well. I would like to go on the record as asking that that classified briefing with staff—bipartisan staff occur. Can I get your commitment on trying to make that happen?

Mr. CHAO. Yes, sir.

Mr. BURGESS. Thank you. So the much-talked-about Red Team discussion document from The Washington Post this morning, which, of course, you have not seen, and I appreciate that, but you were interviewed, in response to Mr. Barton's questions, you were interviewed by the McKinsey team who were developing this?

Mr. CHAO. Yes.

Mr. BURGESS. Do you remember when?

Mr. CHAO. Approximately an April time frame.

Mr. BURGESS. During the time frame that this was being developed. Do you recall what you talked about?

Mr. CHAO. I think primarily what I was intimating to the McKinsey team was a schedule challenge, because during April, we had just started QHP submission, and working with issuers. They were very nervous that——

Mr. BURGESS. Excuse me, what is QHP?

Mr. CHAO. Qualified health plans.

Mr. BURGESS. OK.

Mr. CHAO. I apologize. And in—during that month, it was a rapid, you know, process to collect all the qualified health plan data that you see in plan compare on Healthcare.gov now, as well as in the State-based marketplaces, and I was remarking on how that is unprecedented to only give issuers, you know, that short amount of time to submit their data, and that we needed to make adjustments in the windows potentially so that they could come back in and make corrections. You know, that is an example of what I talked about in terms of the schedule challenges that we were trying to undertake something large-scale, fairly complex compared to what is happening in the insurance landscape today, and that this was new and we were working on a short time frame.

Mr. BURGESS. And I will stipulate that those are legitimate concerns. And so on page 1 of this Red Team document, at the bottom of the page, highlighted, the working group determined that extending the go-live date should not be part of the analysis, and, therefore, work with a boundary condition of October 1 as the launch date. In other words, it didn't matter what the conditions on the ground were, come hell or high water, October 1 we have got to go live. And were you given that impression by anyone on your team as you worked through this?

Mr. CHAO. Not necessarily characterized that way, but as I mentioned——

Mr. BURGESS. Well, let me interrupt you again, my time is limited. Who would have made a decision like that, that it doesn't matter—I mean it is like the old saying, it doesn't matter what—don't check the weather, we are flying anyway. Who would make a decision like that?

Mr. CHAO. I think the decision ultimately is made, you know, by Marilyn Tavenner and, you know, a team of folks, I suppose, that she works with. But as the administrator, she sets the deadlines for my work, and——

Mr. BURGESS. Now, some of the people that are referenced in the report given to the committee by McKinsey, that people that had discussions in the White House, the old Executive Office Building, people like Nancy-Ann DeParle, Jeanne Lambrew, do you know if they were involved in these decisions?

Mr. CHAO. I can't speak to that. I didn't hear anything about those discussions.

Mr. BURGESS. Have you been in meetings with Jeanne Lambrew and Nancy-Ann DeParle?

Mr. CHAO. Yes.

Mr. BURGESS. And what—could you characterize those meetings?

Mr. CHAO. The ones that I remember were dealing with coordination with IRS on their FTI, Federal Tax Information, requirements, security protections and the Privacy Act with SSA.

Mr. BURGESS. At any point during those meetings, did it come up with the concern that we may not be ready trying to integrate all of these moving parts by October 1?

Mr. CHAO. Not in that context, no.

Mr. BURGESS. In any context?

Mr. CHAO. You know, concerns about whether if agencies were working closely together, but not really in the context of October 1, no.

Mr. BURGESS. One of the other things that keeps coming up repeatedly in this report is that, number 1, there were evolving requirements, there wasn't a consistent endpoint, there were multiple definitions of success, and in spite of all of the concerns brought up by the report, it must launch at full volume. I mean it almost sounds like a recipe for disaster, doesn't it? You are changing the definition as it goes along, you are not allowed to change the date, and you have got to launch at full volume. That is a pretty tall order, isn't it?

Mr. CHAO. It is.

Mr. BURGESS. Well, let me ask you this. How does it make you feel to know that there was this kind of report out there, and that other people knew about it, people in the White House, people within the Agency, and you have been the primary point man out there and no one discussed it with you? How does that make you feel?

Mr. CHAO. I am actually not terribly hurt by it or surprised by it. I think the information contained within it is something that I live on a day-to-day basis to try to deliver a working system. I——

Mr. BURGESS. You are playing into everyone's worst fear about what it is like to be in the bureaucracy.

Let me ask you this. One of the things brought up in this report is that there is not a single implementation leader——

Mr. MURPHY. Gentleman's time has expired.

Mr. BURGESS [continuing]. Do you feel during your time that there has been a single implementation leader that you could look to for advice and direction through this?

Mr. CHAO. I think I have looked to several because of how——

Mr. BURGESS. Name one.

Mr. CHAO. Marilyn Tavenner.

Mr. MURPHY. Gentleman's time has expired. We are going to need to follow up with that. So we will submit those questions for the record too.

Now recognize the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. And like all of us, I have some concern, I have some questions in a minute about the Healthcare.gov, but I want to just say that, you know, it is frustrating for those of us on this side of the aisle who supported it, who actually worked a lot of times on the drafting of different versions of the Affordable Care Act, to see what happened on October 1 without the rollout. And to have it successful, that is the way we need to deal with it, because having been here through also the prescription drug plan for seniors, that is the way you can get to the numbers you really need. So hopefully that will happen. But the law is still there, and last Saturday in our district, at least in Houston, because in Texas, we are unfortunate, we have some of the highest percentage and numbers of uninsured folks in the country, and in our congressional district 42 percent of my constituents work and don't have insurance through their employer. So they would be qualified to go with the ACA. And we actually did it by paper. Now, I have to admit, I can't remember except—and I wasn't around when Medicare was rolled out. I guess that was the last time we rolled anything out by paper, but let me give you the results. We had 3 members of Congress, the Mayor of Houston, our Republican county judge, and the Secretary of Labor. We actually had 800 families show up on a Saturday morning and signed in, of course, with multiple attendees per family, nearly 300 people set up follow-up appointments after a navigator. We had 88 of the certified navigators there. And we don't know how many applications were completed because the number is still be tallied by navigators and HHS and our regional office out of Dallas. So there are people out there who want to do it. And if we have to do it by paper, we will do it, but that is the frustration we have. We want this to work because there are millions of people in our country who need this. Now, I know the majority in the House may not understand that, but I know in our district they do.

But I don't know if you have a comment, but let me—and I can get to the Healthcare.gov.

Mr. CHAO. I think CMS takes to heart the matter, and I think everyone working on this is absolutely serious about improving this experience because we know that in districts like yours, there are quite a few number of people that need and want to enroll and use this benefit. So we are certainly working very hard to make that happen.

Mr. GREEN. Well, with that success, believe me, we are going to do a lot of smaller ones in our district, and try and work with them and partner with media companies to maybe get the message out.

I have a few questions about Healthcare.gov and the important goal I think we both share, and sharing is part of the success in implementation of the Affordable Care Act, people can have access to care they need and when they need it. Part of this goal requires that Federal and State exchanges secure the American people can trust their information and privacy won't be compromised. How is

the Data Hub used to determine eligibility and enroll applicants and process appeals different from the data systems used by other Federal agencies, such as Social Security or the IRS?

Mr. CHAO. How is the Data Hub different?

Mr. GREEN. Than the other agencies who obviously have up and running ways where Social Security and even IRS you can file?

Mr. CHAO. Well, I think what makes it different is that, for example, SSA is the eligibility agency for Medicare. So every night, SSA's field offices load data about accretions and deletions into the Medicare Program, and we receive a very large file from them every night that we process for 2 to 3 hours to update all of our systems, so that providers can see new Medicare beneficiaries accreting into the system. That is lots of data moving between 2 organizations, and it is stored and it is time-intensive. The Data Services Hub goes out and, for a requestor of that data, a valid requestor, it reads the data where the source is, transfers it back to the requestor in a secure fashion, does not remember the contents of that data, and facilitates that without moving massive, you know, millions of records of data all at once, all the time, every day. It only transfers enough data to get the job done.

Mr. GREEN. Were you at the HHS when we have gone through two Medicare enrolling by internet? I mean when we shifted from having to go into a Social Security office to file the paperwork, you can do it online now.

Mr. CHAO. Yes. Yes.

Mr. GREEN. And I assume there were some glitches when that first started.

Mr. CHAO. Yes.

Mr. GREEN. And, of course, we didn't have a deadline and a rollout and things like that. It was built in over the time so you had time to problem solve. And——

Mr. CHAO. Right.

Mr. GREEN [continuing]. Our problem is we don't have that time to problem solve here in later November, and——

Mr. CHAO. I still remember in the mid-'90s, SSA put up the electronic benefits statement, and after a few months, they had to take it down and it didn't come back up until years later——

Mr. GREEN. Well——

Mr. CHAO [continuing]. Until they perfected it.

Mr. GREEN. OK, thank you, Mr. Chairman.

Mr. MURPHY. Gentleman yields back.

Now recognize the gentleman from Louisiana, Mr. Scalise, for 5 minutes.

Mr. SCALISE. Thank you, Mr. Chairman. I appreciate you having this hearing, and, Mr. Chao, appreciate you coming to testify before the committee.

We have had a number of hearings like this over the last few months, trying to find out first how the rollout was going to work, and of course, we have gotten testimony time and time again from the administration that the rollout was going to be fine. And then I think what is most frustrating is that when this report came out, this McKinsey report, that really chronicles the problems that were happening months ago, back in March and April, at the same time that administration officials were telling us that everything was

going to be fine, and to that—and telling American families that everything was going to be fine when October 1 hit. I guess there are many things about this that trouble me, but first, you know, when I look at this, you say you hadn't seen this report, and I have read through a number of these items that McKinsey pointed out in the report that they were telling them to somebody in CMS, around you, over you, under you, somewhere, but these are things that should have been just basic testing requirements. I, you know, I used to write software. I actually wrote test plans for software rollouts, and, you know, in fact, many of these are just basic commonsense things you do. I mean we—if we made one line of code change, we literally would test that over and over in multiple ways, let alone major changes.

What this report talks about is chaos at CMS. Nobody is in charge. They talk about the fact that you had multiple people that were making multiple changes to—and major design changes to the system just weeks prior to testing, I mean—prior to the rollout without testing it. I mean did you have a test plan, whether or not you read this report, these are things that you should have been doing anyway. I mean were you all making changes, big changes all the way through, and were you testing any of those changes, or just saying, well, you know, they told us October 1, roll it out no matter what.

Mr. CHAO. You have asked a lot of questions in there.

Mr. SCALISE. Yes.

Ms. CHAO. So let me try to recall how to address them. I think that certainly, yes, if you have this experience in software development, you need to have solid requirements before you can actually have good test cases in which to actually run tests. I think it is a dynamically changing environment of which, if we had more time and that time would have been devoted to solidifying requirements that are translated from policy——

Mr. SCALISE. You had 3 years. I mean there were 3 years. This is not something that just kind of got plopped on your desk. I mean the law passed and was signed into law in 2010. There was a lot of time to prepare for it. The requirements—the major requirements were changing weeks before, some of them for political reasons by the Obama administration. So you can't just say, well, you know, we just didn't have enough time. I mean somebody in CMS, and if it wasn't you, it was—maybe it was Ms. Tavenner or who knows who it was, but somebody was making all these changes and saying, gee whiz, I mean, you know, we—let us make big changes and don't test it because we just want to roll this thing out no matter what.

Mr. CHAO. Well, having written software or written test cases, you know that the requirements come from the business side or the policy side. And they are subject to change based upon how your customer or your business——

Mr. SCALISE. The law didn't change.

Mr. CHAO. I——

Mr. SCALISE. The law was passed, and for 3 years that law didn't change. The law was there. You knew what those requirements were. Now, if you make changes in the requirements, you also ought to make changes in your test plan.

Mr. CHAO. I think the law has a very high-level expression of requirements that, certainly, you can't develop code or test cases from. There needs to be a significant amount of translation into lower level details. And that is what I mean by a schedule, challenges that we have to receive those requirements and translate them into test cases, test data, to exercise the system as well as build the system too. So——

Mr. SCALISE. All right, well, look, they talk in this report that the contractor received absolutely conflicting direction between the various entities within CMS. Conflicting directions within CMS. That is not a requirement change. That is one person saying do this, and another person in the same agency saying do something different. And, by the way, none of that is being tested in the meantime. That is not evolving requirements, that is chaos within the Obama administration where they are literally changing things and multiple people are changing them and nobody is talking to anybody.

Mr. CHAO. Well, I can't speak to how they characterized it, but I think that in CMS, we have Medicaid and CHIP requirements, we have insurance exchange requirements, oversight requirements, medical loss ratio, rate review, early retiree reinsurance, pre-existing——

Mr. SCALISE. And I know you all have that. Look——

Mr. CHAO. There are lots of——

Mr. SCALISE [continuing]. You have got a job to——

Mr. CHAO [continuing]. All I am saying is——

Mr. SCALISE. The bottom line is, the bottom line is, you know, this report lays out the chaos that was going on, but all of this information was known within the White House. Reports were being briefed to people in the White House. And either President Obama didn't know about it, in which case people directly under him knew that this thing was going to be a disaster and just didn't tell him, or the President did know about it and went out misleading people anyway. But either way, if the President really didn't know about this, this report says the White House absolutely knew what was going on, and they didn't tell the President. He ought to be firing these people today. If somebody—if a CEO went out there and said I am rolling out this project, this would be just like buying a TV on Amazon, that is what the President said, and if somebody right underneath him knew that it wasn't going to be like that, and this report says absolutely they knew and they didn't tell the President, he ought to go and fire every single one of those people right now and hold them accountable, or maybe that just says that he did know about it. And we will see what the President says, but this report is damming.

And I yield back the balance of my time.

Mr. MURPHY. Gentleman's time has expired.

Just—can you just clarify an answer you gave to the gentleman here? I thought you said something like, with more time, you would have done more testing, or something along those lines. Are you saying you would have liked to have more time?

Mr. CHAO. No, I think that is what I mean by there is a schedule, challenges that you are trying to maximize the time that you have left, as you are trying to extract the requirements from the

policy that is being finalized. The longer a policy takes to be finalized, the longer it takes to translate the——

Mr. MURPHY. Do you wish you would have had more time to test it?

Mr. CHAO. I think that is true of every project I have ever worked on.

Mr. MURPHY. Thank you.

Now recognize Mr. Yarmuth for 5 minutes.

Mr. YARMUTH. Thank you, Mr. Chairman. Thank you, Mr. Chao, for your testimony today.

I just want to follow up a little bit on Mr. Scalise's line of questioning, the issue of whether or not you had 3 years to prepare for this. When was the deadline for States to decide when they're—they were joining the—doing their own Exchanges or were going to participate in the Federal Exchange?

Mr. CHAO. I think the time frame was the end of 2012.

Mr. YARMUTH. End of 2012. So January 1, essentially, of this past year. And when was the deadline for States to decide whether they were going to enter into a partnership with the Federal Government?

Mr. CHAO. I believe it was the end of April of 2013.

Mr. YARMUTH. So really, the department did—or CMS did not have 3 years to prepare, and there was probably no way to guess 3 years ago that only 14 States and the District of Columbia were going to set up their own Exchanges. Wasn't the anticipation that far more States would do their own Exchanges?

Mr. CHAO. Yes, we were hoping so.

Mr. YARMUTH. So it really wasn't until this year that CMS really understood the magnitude of the volume of work that the Web site was going to have to accommodate?

Mr. CHAO. Correct. It is——

Mr. YARMUTH. Right.

Mr. CHAO [continuing]. Not such a clear binary decision. You do or you don't. There is still coordination that has to occur in——

Mr. YARMUTH. Right. Thank you for that.

Now, obviously, when we are talking about security, we are talking about two separate issues; one is the vulnerability of the system to some kind of outside attack. I don't know why anyone would really want to attack the Federal Exchange, but assuming that is an issue. The second one is, the average citizen is concerned about information that is there about them. And I think that is one thing we are most interested here. Mr. Dingell actually asked you directly about the fact that there really isn't very much information on the Web site that would be considered private in nature. And I guess the question I would ask is, are people who are working with the Exchange now subject to or vulnerable to a more of a breach of their privacy than they were under the prior system when the insurance companies had pages and pages and pages of health information, including every doctor they had ever visited, every prescription they had ever taken, every medical procedure they had undergone and—over a certain period of time? Would you say that there was much more vulnerability under that system than there would be under the Federal Exchange?

Mr. CHAO. Much more so because so much more personal information, including health information, was involved in that process.

Mr. YARMUTH. And I think during the course of questioning we have actually done a pretty good job of debunking the issue as to whether there really was security problem here. There is no evidence that there has been, and I think there really hasn't been any evidence presented that would make us doubt that. So I am glad about that, and I think that should encourage Americans to participate more actively.

And since—one other thing that has come up, and it involves the question of 80 percent, and it is something I want to clarify because the press reports have been that the administration has said as a metric that 80 percent will be able to get on the site and smoothly sign up—enroll for health coverage as of the end of this month. That doesn't mean that the remaining 20 percent won't be able to access affordable quality health insurance, does it?

Mr. CHAO. No. I can't speak to the exact percentages, but I think there is a recognition that some people, whether it be Healthcare.gov or any system, for example, if you walked into an SSA field office, how many people can actually get their business done in one visit, as compared to, you know, the greater majority of people? I think some people need extra help. They need assistance to navigate the process, and I think that that is probably what they were referring to.

Mr. YARMUTH. Thank you very much for that.

And I just want to do some shameless self-promotion for my State right now. As of last Friday, Kentucky, obviously operating its own Exchange, 48,000 Kentuckians are enrolled in new health insurance, 41 percent of them are under the age of 35. Over 452,000 visitors have gone to the Web site, 380,000 people have conducted preliminary screenings to find out if they are eligible for coverage. And I think most importantly maybe, over—almost 1,000 businesses have actually begun the process of signing up for new coverage for their employees, and over 300 have actually been enrolled and have been qualified now to offer coverage. So Kentucky is doing well, and I hope the Federal Exchange will do just as well.

I yield back.

Mr. MURPHY. Gentleman yields back.

Now recognize Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman. And, Mr. Chao, thank you for your time here today.

And you replied earlier on a follow-up question that the chairman had, I believe you said you would have liked to have had more time for the testing. Did you request more time from anyone?

Mr. CHAO. No.

Mr. HARPER. And can you tell me why you did not request more time?

Mr. CHAO. Because I was given a target of October 1 and various other deliver dates, of which I had to stay on schedule for.

Mr. HARPER. Did you believe it was ready for October 1?

Mr. CHAO. I believe we did everything we could to make sure that the right priorities were set so that we could deliver a system on October 1.

Mr. HARPER. And do you believe the system was delivered on October 1?

Mr. CHAO. It was.

Mr. HARPER. Do you believe——

Mr. CHAO. It wasn't performing as well as we liked, and certainly had more glitches than we anticipated, but we did deliver a system on October 1.

Mr. HARPER. Do you think glitches is the proper word to use to describe the rollout?

Mr. CHAO. I think there are problems. There are defects if you—you know, glitches is just a word that is commonly used right now.

Mr. HARPER. Well, glitches doesn't seem to convey how serious the failure of the rollout has been, and so here we are. And, of course, one of the big concerns that we have is what do you do about making sure that personally identifiable information for those who sign up is protected. And on the report that you have there, on page 11, if I could get you to take a look at that real quick. On the McKinsey report. At the bottom of page 11 it says—and, of course, at the top it says, options that could be implemented to help mitigate key risks. At the bottom it says, name a single implementation leader and implement associated Government process. Has there been a single implementation leader named?

Mr. CHAO. I don't think that is the way it has been characterized before by, I think, Marilyn Tavenner, our administrator, certainly has accepted accountability and she does run the agency and——

Mr. HARPER. Certainly, but that is not saying that she is supposed to be the single implementation leader there. Is that how you read that report?

Mr. CHAO. I—but again, I didn't see this until just this very minute, so I——

Mr. HARPER. All right, when—you know, I spent some time here while we were waiting on time to question here, I went to the Healthcare.gov site, and it took a little while to try to figure out how in the search to get to the information on how you protect yourself from fraud in the health insurance marketplace. And it takes a couple of steps to get to this information. So people probably more sophisticated than I am on this would need to be tracking this. But if you look at it on the site, it says how to report suspected fraud, and it said you can report suspected fraud in one of two ways, and it lists a breakdown of one way, which is to use the Federal Trade Commission's online complaint assistant. And I tried that a moment ago and it was not very successful. It says you can call your local police department, and then it says you can visit a site, the Federal Trade Commission, to learn more about identity theft. And the second choice is to call the Health Insurance Marketplace Call Center, and it gives that number. So if you were the victim of personally identifiable information being fraudulently released or obtained, who would you call first under that scenario?

Mr. CHAO. The listed call center number. The marketplace call center.

Mr. HARPER. And it——

Mr. CHAO. If you are in a Federally Facilitated Marketplace.

Mr. HARPER. OK, and it says, explain what happened and your information will be handled appropriately. How do you define handled appropriately? What is that? How do you get someone's identity back once it has been compromised or there has been an identity theft?

Mr. CHAO. Well, I think there needs to be some analysis and collection of information to make sure what type of situation occurred, and then make a decision going forward there.

Mr. HARPER. Well, obviously, this is a critical matter, so some determination made. What is the time frame? How quickly can someone's life be put back together if this were to happen?

Mr. CHAO. I think it is situationally dependent, and I really can't—I am not comfortable——

Mr. HARPER. Sure.

Mr. CHAO [continuing]. Giving you an answer right off——

Mr. HARPER. You had said earlier that steps were being taken to prevent unauthorized access to the site. What about those who may have authorized access but release it in an unauthorized manner, what protections or safeguards are put in there particularly for those that are the navigators, and the situation that there has been no background check, unless it was required in the State, how is that being handled with the use of navigators?

Mr. CHAO. I think the premise is that when we issue, for example, a grant to a navigator organization, or we sign a computer matching agreement with a State, that there are rules of behavior and certain, you know, kinds of requirements that are associated with signing that agreement or receiving that grant.

Mr. HARPER. Do you have a central reporting location of the navigators that are in violation or reported in violation?

Mr. CHAO. I have to check on that.

Mr. HARPER. My time has——

Mr. MURPHY. Gentleman's time has expired.

Mr. HARPER. You let us know. My time has expired.

Mr. MURPHY. Thank you.

Mr. Lujan is recognized for 5 minutes.

Mr. LUJAN. Mr. Chairman, thank you so very much.

Mr. Chao, you were just presented with a whole series of hypotheticals. Have any of those hypotheticals happened?

Mr. CHAO. No, not to our knowledge, no.

Mr. LUJAN. I appreciate that, and I would suggest, Mr. Chao, if someone was maliciously using information in a way that they were not allowed to use it, would that be a crime?

Mr. CHAO. Can you repeat that question again?

Mr. LUJAN. If someone hacked into the Web site, and was using information in a way that they weren't allowed to use it, so—and anyway, wouldn't that be considered a crime?

Mr. CHAO. Certainly, yes.

Mr. LUJAN. And I believe that we could fully prosecute those individuals?

Mr. CHAO. Yes.

Mr. LUJAN. And I would hope that this committee would fully support and encourage the Department of Justice to go and fully prosecute anyone that is hacking this Web site.

Mr. Chairman, it wasn't too long ago that there was a hearing that this committee had on Lifeline, and some of my Republican colleagues were encouraging members—citizens of the United States to go to visit Obamaphone.net to sign up for a Lifeline or to get information from the Web site as to the accuracy of what the program was about. An hour later, the Web site was taken down, and this committee, myself and Congresswoman Eshoo, asked the FTC to look into the matter, but they said it appears that in the fraudulent way that this data was being collected, that the Web site is now down.

I think we as Members of Congress need to be careful with how we are purporting information out to the American people. We need to be careful about this. There is not, again, a member on this committee that doesn't believe that we should get the Web site working, that we need to get to the facts of what is happening. And with that being said, Mr. Chao, I guess two things. Mr. Chairman, there is GAO report that was published on April 24 of 2012, entitled "Cybersecurity, Threats Impacting the Nation," and I would like to ask unanimous consent to insert it into the record.

Mr. MURPHY. Sure.

Mr. LUJAN. The report, and I would invite everyone in the committee to take a look at this. It was to the Homeland Security Department or committee, talking about the threats that our Nation is facing. The intelligence community, Homeland Security, the White House, members of Congress Web sites that have been hacked into. We need to do more in this area to make sure that we are keeping information secure.

But with that being said, Mr. Chao, this has been talked about a bit, but on the front page of The Washington Post this morning, there was an article about a document that was leaked to the paper by the committee majority. The article describes an analysis conducted in 2013 by McKinsey and Company that identified potential risks in the development of Healthcare.gov. The report shadowed some of the problems that we now face today.

Mr. Chao, did you see the report at the time it was published in March and April of 2013?

Mr. CHAO. No, I did not.

M. LUJAN. So is it fair to say that you are not the best person to comment on why the report was done, and how CMS and HHS responded to its findings?

Mr. CHAO. Yes.

Mr. LUJAN. Mr. Chairman, I raise this because it illustrates a number of problems with how this has been handled. In particular, the perception that is created when you withhold documents from the Democrats on the committee, and when you play gotcha games by leaking material to the press without context, it makes it appear that you are more interested in running a partisan investigation than in finding the facts, and I certainly hope that that is not the case, and believe that not to be true, but we need to work together to get to the bottom of this.

So with that being said, Mr. Chao, what efforts is the Department of Health and Human Services undertaking to address the ongoing threats?

Mr. CHAO. We listed as part of our mitigation strategy daily and weekly security testing and scans, which is something we always do, but in this case we do it more frequently because we understand the sensitive nature of Healthcare.gov and the trust that—and confidence we have to obtain from people to come and use the site.

Mr. LUJAN. And how is the department coordinating with other Federal agencies who maintain Web sites that also gather personal information?

Mr. CHAO. I think we work with all of our key partners that are connected to the Hub to make sure that we function under what we call a harmonized privacy and security framework, and along with the States, have a process and a program in place to handle certain situations of which there are incidents that need to be managed, about potential data breaches. So we have a program, we have a policy, we have a set of operational procedures in place, working and coordinating across all these agencies.

Mr. LUJAN. And does that include, Mr. Chao, the intelligence community, the Department of Homeland Security?

Mr. CHAO. Yes.

Mr. LUJAN. Very good.

So with that, Mr. Chairman, as I yield back my time, I just hope that it is clear, Mr. Chao, to you, to the President, that we are not happy with the rollout right now. We need to get this working. There are too many vulnerable Americans that need access to care, and we need to make sure that we can get them that coverage, in the same way, protect the information. But I think it is a big step forward that no longer will individuals have to report the kind of illnesses or accidents that they have had in their past, so that they can get care in the future.

And with that, Mr. Chairman, I yield back.

Mr. MURPHY. Gentleman yields back.

And without objection, the gentleman's document will be admitted to the record.

[The information follows:]

United States Government Accountability Office

GAO

Testimony

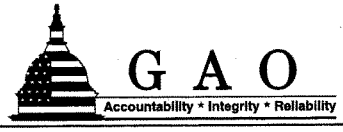
Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, April 24, 2012

CYBERSECURITY

Threats Impacting the Nation

Statement of Gregory C. Wilshusen, Director
Information Security Issues



GAO-12-666T

GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-666T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives

April 24, 2012

CYBERSECURITY

Threats Impacting the Nation

Why GAO Did This Study

Nearly every aspect of American society increasingly depends upon information technology systems and networks. This includes increasing computer interconnectivity, particularly through the widespread use of the Internet as a medium of communication and commerce. While providing significant benefits, this increased interconnectivity can also create vulnerabilities to cyber-based threats. Pervasive and sustained cyber attacks against the United States could have a potentially devastating impact on federal and nonfederal systems, disrupting the operations of governments and businesses and the lives of private individuals. Accordingly, GAO has designated federal information security as a governmentwide high-risk area since 1997, and in 2003 expanded it to include protecting systems and assets vital to the nation (referred to as critical infrastructures).

GAO is providing a statement that describes (1) cyber threats facing the nation's systems, (2) vulnerabilities present in federal information systems and systems supporting critical infrastructure, and (3) reported cyber incidents and their impacts. In preparing this statement, GAO relied on previously published work in these areas and reviewed more recent GAO, agency, and inspectors general work, as well as reports on security incidents.

What GAO Recommends

GAO has previously made recommendations to resolve identified significant control deficiencies.

View GAO-12-666T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The nation faces an evolving array of cyber-based threats arising from a variety of sources. These threats can be intentional or unintentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems, and intentional threats can be both targeted and untargeted attacks from a variety of threat sources. Sources of threats include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Moreover, potential threat actors have a variety of attack techniques at their disposal, which can adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. The nature of cyber attacks can vastly enhance their reach and impact due to the fact that attackers do not need to be physically close to their victims and can more easily remain anonymous, among other things. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals, businesses, critical infrastructures, or government organizations.

The threat posed by cyber attacks is heightened by vulnerabilities in federal systems and systems supporting critical infrastructure. Specifically, significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems supporting the operations, assets, and personnel of federal government agencies. For example, 18 of 24 major federal agencies have reported inadequate information security controls for financial reporting for fiscal year 2011, and inspectors general at 22 of these agencies identified information security as a major management challenge for their agency. Moreover, GAO, agency, and inspector general assessments of information security controls during fiscal year 2011 revealed that most major agencies had weaknesses in most major categories of information system controls. In addition, GAO has identified vulnerabilities in systems that monitor and control sensitive processes and physical functions supporting the nation's critical infrastructures. These and similar weaknesses can be exploited by threat actors, with potentially severe effects.

The number of cybersecurity incidents reported by federal agencies continues to rise, and recent incidents illustrate that these pose serious risk. Over the past 6 years, the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent. These incidents include unauthorized access to systems; improper use of computing resources; and the installation of malicious software, among others. Reported attacks and unintentional incidents involving federal, private, and infrastructure systems demonstrate that the impact of a serious attack could be significant, including loss of personal or sensitive information, disruption or destruction of critical infrastructure, and damage to national and economic security.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the cyber-based threats facing our nation.

The increasing dependency upon information technology (IT) systems and networked operations pervades nearly every aspect of our society. In particular, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependency can also create vulnerabilities to cyber-based threats. Pervasive and sustained cyber attacks against the United States could have a potentially devastating impact on federal and nonfederal systems and operations. In January 2012, the Director of National Intelligence testified that such threats pose a critical national and economic security concern.[1] These growing and evolving threats can potentially affect all segments of our society—individuals; private businesses; local, state, and federal governments; and other entities. Underscoring the importance of this issue, we have designated federal information security as a high-risk area since 1997 and in 2003 expanded this area to include protecting computerized systems supporting our nation's critical infrastructure.[2]

In my testimony today, I will describe (1) cyber threats facing the nation's systems, (2) vulnerabilities present in federal systems and systems supporting critical infrastructure,[3] and (3) reported cyber incidents and their impacts. In preparing this statement in April 2012, we relied on our previous work in these areas. (Please see the related GAO products in appendix I.) These products contain detailed overviews of the scope and methodology we used. We also reviewed more recent agency, inspector

[1]James R. Clapper, Director of National Intelligence, Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence (January 31, 2012).

[2]See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[3]Critical infrastructures are systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on national security, economic well-being, public health or safety, or any combination of these.

general, and GAO assessments of security vulnerabilities at federal agencies and information on security incidents from the U.S. Computer Emergency Readiness Team (US-CERT), media reports, and other publicly available sources. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, as well as developing into an extended information and communications infrastructure supporting vital services such as power distribution, health care, law enforcement, and national defense.

Consequently, the security of these systems and networks is essential to protecting national and economic security, public health and safety, and the flow of commerce. Conversely, ineffective information security controls can result in significant risks, including

- loss or theft of resources, such as federal payments and collections;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personal taxpayer information, or proprietary business information;
- disruption of critical operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government; and
- use of computer resources for unauthorized purposes or to launch attacks on other computers systems.

The Nation Faces an Evolving Array of Cyber-Based Threats

Cyber-based threats are evolving and growing and arise from a wide array of sources. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Table 1 shows common sources of cyber threats.

Table 1: Sources of Cybersecurity Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.

Threat source	Description
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

These sources of cyber threats make use of various techniques, or exploits, that may adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Table 2 provides descriptions of common types of cyber exploits.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bombs	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.

Type of exploit	Description
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer– sometimes with a powerful antenna–searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

The unique nature of cyber-based attacks can vastly enhance their reach and impact. For example, cyber attackers do not need to be physically close to their victims, technology allows attacks to easily cross state and national borders, attacks can be carried out at high speed and directed at a number of victims simultaneously, and cyber attackers can more easily remain anonymous. Moreover, the use of these and other techniques is becoming more sophisticated, with attackers using multiple or "blended" approaches that combine two or more techniques. Using these techniques, threat actors may target individuals, resulting in loss of privacy or identity theft; businesses, resulting in the compromise of proprietary information or intellectual capital; critical infrastructures, resulting in their disruption or destruction; or government agencies, resulting in the loss of sensitive information and damage to economic and national security.

Systems Supporting Federal Operations and Critical Infrastructure Are Vulnerable to Cyber Attacks

Significant weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. For example, in their performance and accountability reports and annual financial reports for fiscal year 2011, 18 of 24 major federal agencies[4] indicated that inadequate information security controls were either material weaknesses or significant deficiencies[5] for financial reporting purposes. In addition, inspectors general at 22 of the major agencies identified information security or information system control as a major management challenge for their agency.

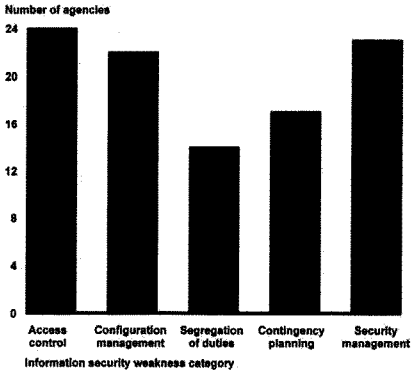
Agency, inspectors general, and GAO assessments of information security controls during fiscal year 2011 revealed that most major federal agencies had weaknesses in most of the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which helps avoid significant disruptions in computer-dependent operations; and (5) agencywide information security programs, which provide a framework for ensuring that risks are understood and that effective controls are selected and implemented. Figure 1 shows the

[4]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[5]A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

number of agencies that had vulnerabilities in these five information security control categories.

Figure 1: Information Security Weaknesses at 24 Major Federal Agencies in Fiscal Year 2011



Source: GAO analysis of agency, inspectors general, and GAO reports.

Over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve similar previously identified significant control deficiencies. We have also recommended that agencies fully implement comprehensive, agencywide information security programs, including by correcting weaknesses in specific areas of their programs. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, securing the control systems that monitor and control sensitive processes and physical functions supporting many of our nation's critical infrastructures is a national priority, and we have identified vulnerabilities in these systems. For example, in September 2007, we reported that critical infrastructure control systems faced increasing risks due to cyber threats, system vulnerabilities, and the serious potential

impact of possible attacks.[6] Specifically, we determined that critical infrastructure owners faced both technical and organizational challenges to securing control systems, such as limited processing capabilities and developing compelling business cases for investing in control systems security, among others. We further identified federal initiatives under way to help secure these control systems, but noted that more needed to be done to coordinate these efforts and address shortfalls. We made recommendations to the Department of Homeland Security to develop a strategy for coordinating control systems security efforts and enhance information sharing with relevant stakeholders. Since this report, the department formed the Industrial Control Systems Cyber Emergency Response Team to provide industrial control system stakeholders with situational awareness and analytical support to effectively manage risk. In addition, it has taken several actions, such as developing a catalog of recommended security practices for control systems, developing a cybersecurity evaluation tool that allows asset owners to assess their control systems and overall security posture, and collaborating with others to promote control standards and system security. We have not evaluated these activities to assess their effectiveness in improving the security of control systems against cyber threats.

In May 2008, we reported that the Tennessee Valley Authority's (TVA) corporate network contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[7] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA's critical infrastructures and 73 recommendations to address weaknesses in information security controls. TVA concurred with the recommendations and has taken steps to implement them.

In addition to those present in federal systems and systems supporting critical infrastructure, vulnerabilities in mobile computing devices used by individuals or organizations may provide openings to cyber threats. For example, consumers and federal agencies are increasing their use of mobile devices to communicate and access services over the Internet.

[6]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

[7]GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

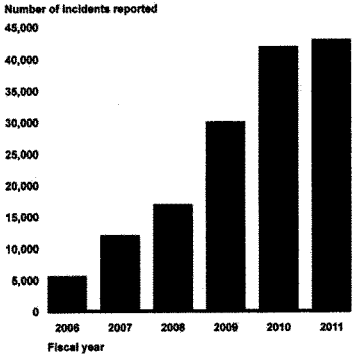
The use of these devices offers many benefits including ease of sending and checking messages and remotely accessing information online; however, it can also introduce information security risks if not properly protected. We have ongoing work to determine (1) what common security threats and vulnerabilities affect generally available cellphones, smartphones, and tablets; (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities; and (3) the extent to which government and private entities are addressing security vulnerabilities of mobile devices.

Number of Cybersecurity Incidents Reported by Federal Agencies Continues to Rise, and Recent Incidents Illustrate Serious Risk

Federal agencies have reported increasing numbers of security incidents that placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. When incidents occur, agencies are to notify the federal information security incident center—US-CERT. Over the past 6 years, the number of incidents reported by federal agencies to US-CERT has increased from 5,503 incidents in fiscal year 2006 to 42,887 incidents in fiscal year 2011, an increase of nearly 680 percent (see fig. 2).[8]

[8]According to US-CERT, the growth in the number of incidents is attributable, in part, to agencies improving detection and reporting of security incidents on their respective networks.

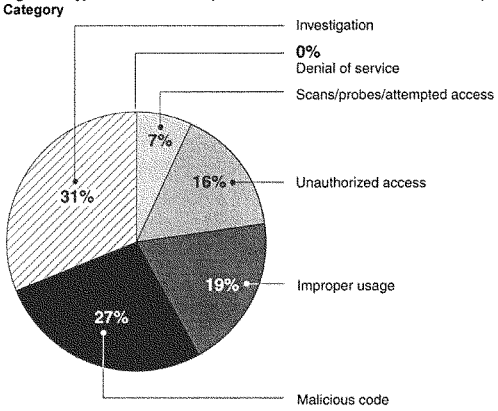
Figure 2: Incidents Reported to US-CERT: Fiscal Years 2006-2011



Source: GAO analysis of US-CERT data for fiscal years 2006-2011.

Agencies reported the types of incidents and events based on US-CERT-defined categories. As indicated in figure 3, the two most prevalent types of incidents and events reported to US-CERT during fiscal year 2011 were unconfirmed incidents under investigation and malicious code.

Figure 3: Types of Incidents Reported to US-CERT in Fiscal Year 2011 by Category



GAO analysis of US-CERT data for fiscal year 2011.

Reported attacks and unintentional incidents involving federal, private, and critical infrastructure systems demonstrate that the impact of a serious attack could be significant. These agencies and organizations have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples from news media and other public sources illustrate that a broad array of information and assets remain at risk.

- In April 2012, hackers breached a server at the Utah Department of Health to access thousands of Medicaid records. Included in the breach were Medicaid recipients and clients of the Children's Health Insurance Plan. About 280,000 people had their Social Security numbers exposed. In addition, another 350,000 people listed in the eligibility inquiries may have had other sensitive data stolen, including names, birth dates, and addresses.
- In March 2012, it was reported that a security breach at Global Payments, a firm that processed payments for Visa and Mastercard, could compromise the credit- and debit-card information of millions of Americans. Subsequent to the reported breach, the company's stock

fell more than 9 percent before trading in its stock was halted. Visa also removed the company from its list of approved processors.

- In February 2012, the inspector general at the National Aeronautics and Space Administration testified that an unencrypted notebook computer had been stolen from the agency in March 2011. The theft resulted in the loss of the algorithms used to command and control the International Space Station.
- In March 2012, a news wire service reported that the senior commander of the North Atlantic Treaty Organization (NATO) had been the target of repeated cyber attacks using the social networking website Facebook that were believed to have originated in China. According to the article, hackers repeatedly tried to dupe those close to the commander by setting up fake Facebook accounts in his name in the hope that his acquaintances would make contact and answer private messages, potentially divulging sensitive information about the commander or themselves.
- In March 2012, it was reported that Blue Cross Blue Shield of Tennessee paid out a settlement of $1.5 million to the U.S. Department of Health and Human Services arising from potential violations stemming from the theft of 57 unencrypted computer hard drives that contained protected health information of over 1 million individuals.
- In January 2012, the Department of Commerce discovered that the computer network of the department's Economic Development Administration (EDA) was hit with a virus, forcing EDA to disable e-mail services and Internet access pending investigation into the cause and scope of the problem, which persisted for over 12 weeks.
- In June 2011, a major bank reported that hackers had broken into its systems and gained access to the personal information of hundreds of thousands of customers. Through the bank's online banking system, the attackers were able to view certain private customer information.
- Citi reissued over 200,000 cards after a May 2011 website breach. About 360,000 of its approximately 23.5 million North American card accounts were affected, resulting in the potential for misuse of cardholder personal information.
- In April 2011, Sony disclosed that it suffered a massive breach in its video game online network that led to the theft of personal information, including the names, addresses, and possibly credit card data belonging to 77 million user accounts.
- In February 2011, media reports stated that computer hackers had broken into and stolen proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.
- In July 2010, a sophisticated computer attack, known as Stuxnet, was discovered. It targeted control systems used to operate industrial

processes in the energy, nuclear, and other critical sectors, reportedly causing physical damage. It is designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.

- A retailer reported in May 2011 that it had suffered a breach of its customers' card data. The company discovered tampering with the personal identification number (PIN) pads at its checkout lanes in stores across 20 states.
- In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

These incidents illustrate the serious impact that cyber threats can have on federal agency operations, the operations of critical infrastructures, and the security of sensitive personal and financial information.

In summary, the cyber-threats facing the nation are evolving and growing, with a wide array of potential threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities. The danger posed by these threats is heightened by the weaknesses that continue to exist in federal information systems and systems supporting critical infrastructures. Ensuring the security of these systems is critical to avoiding potentially devastating impacts, including loss, disclosure, or modification of personal or sensitive information; disruption or destruction of critical infrastructure; and damage to our national and economic security.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Michael Gilmore and Anjalique Lawrence (Assistant Directors), Kristi C. Dorsey, and Lee A. McCracken.

Appendix I: Related GAO Products

Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures. GAO-12-424R. Washington, D.C.: April 13, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO-12-361. Washington, D.C.: March 23, 2012.

Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data. GAO-12-393. Washington, D.C.: March 16, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid. GAO-12-507T. Washington, D.C.: February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. GAO-12-92. Washington, D.C.: December 9, 2011.

Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination. GAO-12-8. Washington, D.C.: November 29, 2011.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. GAO-12-130T. Washington, D.C.: October 6, 2011.

Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. GAO-12-137. Washington, D.C.: October 3, 2011.

Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards. GAO-11-751. Washington, D.C.: September 20, 2011.

Information Security: FDIC Has Made Progress, but Further Actions Are Needed to Protect Financial Data. GAO-11-708. Washington, D.C.: August 12, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. GAO-11-865T. Washington, D.C.: July 26, 2011.

Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities. GAO-11-75. Washington, D.C.: July 25, 2011.

Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain. GAO-11-149. Washington, D.C.: July 8, 2011.

Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate. GAO-11-605. Washington, D.C.: Jun 28, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems. GAO-11-463T. Washington, D.C.: March 16, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. GAO-11-117. Washington, D.C.: January 12, 2011.

Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk. GAO-11-43. Washington, D.C.: November 30, 2010.

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. GAO-11-24. Washington, D.C.: October 6, 2010.

Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems. GAO-10-916. Washington, D.C.: September 15, 2010.

Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies. GAO-10-872T. Washington, D.C.: July 22, 2010.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628. Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.

Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development. GAO-10-466. Washington, D.C.: June 3, 2010.

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. GAO-10-513. Washington, D.C.: May 27, 2010.

Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements. GAO-10-202. Washington, D.C.: March 12, 2010.

Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. GAO-10-237. Washington, D.C.: March 12, 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO-10-338. Washington, D.C.: March 5, 2010.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Mr. MURPHY. The Chair now recognizes the gentleman from Colorado, Mr. Gardner, for 5 minutes.

Mr. GARDNER. Thank you, Mr. Chairman, and thank you, Mr. Chao, for your time before the committee today.

Last week, the President met with several representatives of the insurance industry to discuss solutions that may be possible in light of the Healthcare.gov debacle. Have you had any conversations about changes you can make to Healthcare.gov to assist the insurance industry?

Mr. CHAO. I think part of the strategy—I haven't spoken to the issues myself or been part of those meetings, but I think as part of the strategy under Jeff Zients is to improve the experience of consumers, but that involves, you know, key third parties that are also key to this equation of getting around those agents and brokers, and working with issuers to fix, you know, certain aspects of the systems to make it work better.

Mr. GARDNER. So have you had any discussions then about providing insurance companies with the ability to directly enroll, or anybody in your agency department?

Mr. CHAO. We had designed something called direct enrollment into Healthcare.gov, or part of that FFM system architecture to accommodate that.

Mr. GARDNER. And so that is ready—that feature has been turned on or it has not been turned on?

Mr. CHAO. It was not working well initially, like many other things, but we have been performing fixes and optimizing it, and working with issuers to get direct enrollment up.

Mr. GARDNER. So have you had any discussions about giving insurers direct access to information on eligibility for subsidies?

Mr. CHAO. Only at—in terms of the result. There is a series of——

Mr. GARDNER. That is a——

Mr. CHAO [continuing]. Security and of handoffs.

Mr. GARDNER [continuing]. Yes——

Mr. CHAO. Right.

Mr. GARDNER. That is a yes then?

Mr. CHAO. Yes.

Mr. GARDNER. OK. Thank you for that.

Do you—going back to the question then about the feature on the Web site, will that happen in the future then to that question, discussions about giving insurers direct access to information on eligibility for subsidies? Do you believe that will happen in the future?

Mr. CHAO. It is not really direct access, it is more of a hand-off, a secure hand-off in which they have collected enough information about the applicant and their, you know, or an agent and broker, and this person has given authorization for a consent to work with them as a third party.

Mr. GARDNER. So that is a yes then again as well?

Mr. CHAO. It is not access direct to eligibility data, it is a more involved process that protects the person's information.

Mr. GARDNER. But the insurance company will be getting the subsidy access?

Mr. CHAO. They don't get to calculate it. We—that is a marketplace——

Mr. GARDNER. But they will have information on the eligibility for the subsidies directly?

Mr. CHAO. Only as a result of the marketplace handling that data, not touching that eligibility data themselves.

Mr. GARDNER. The committee has been reviewing materials that indicates that some parts of Healthcare.gov were not completed before the launch, as we have discussed here. What portion or percentage of the Web site remained to be created when you launched on October 1?

Mr. CHAO. I don't have an exact percentage. I think some of previous conversations when people ask about whether things were complete, I look at it in terms of overall marketplace systems——

Mr. GARDNER. So you have never talked about what is complete, what is not complete, whether it is—how much to go?

Mr. CHAO. I think it was a set of priority functions that needed to be in place. Like, for example, you had to authenticate an individual. That is a key function that had to be done.

Mr. GARDNER. Well, how much do we have to build today still? I mean what do we need to build, 50 percent, 40 percent, 30 percent?

Mr. CHAO. I think it is, just an approximation, we are probably sitting somewhere between 60 and 70 percent, because we still have to build the system——

Mr. GARDNER. But 60 or 70 percent that needs to be built still?

Mr. CHAO. Because we still have to build the payment systems to make payments to issuers in January.

Mr. GARDNER. So let me get this correct, 60 to 70 percent of Healthcare.gov still needs to be built?

Mr. CHAO. It is not really Healthcare.gov; it is the Federally Facilitated Marketplace——

Mr. GARDNER. But the entire system that the American people are being required to rely upon——

Mr. CHAO. That part is there.

Mr. GARDNER [continuing]. Sixty to 70 percent——

Mr. CHAO. Healthcare.gov, the online application, verification, determination——

Mr. GARDNER. That is——

Mr. CHAO [continuing]. Plan compare, getting enrolled, generating the enrollment transaction, that is 100 percent there. What I am talking about is——

Mr. GARDNER. But the entire system is 60 to 70 percent away from being complete?

Mr. CHAO. Yes, there is the back office systems, the accounting systems, the——

Mr. GARDNER. Thank——

Mr. CHAO [continuing]. Payment systems——

Mr. GARDNER. Thank you for that.

Mr. CHAO [continuing]. They still need to be——

Mr. GARDNER. And how—of those 60 to 70 percent of systems that are still being built, how are they going to be tested?

Mr. CHAO. You mean the remaining——

Mr. GARDNER. Yes.

Mr. CHAO [continuing]. Thirty to 40 percent? How are they going to be tested?

Mr. GARDNER. Yes.

Mr. CHAO. In the same exact manner we tested everything else.

Mr. GARDNER. Is it difficult to review the new parts of the Web site while it is operating?

Mr. CHAO. It won't affect the front end—the front part——

Mr. GARDNER. But that is pretty difficult, isn't it?

Mr. CHAO. Excuse me?

Mr. GARDNER. It is pretty difficult to review it while it is in operation, correct?

Mr. CHAO. No, it doesn't involve the front part. The——

Mr. GARDNER. Right, but where it is operating within——

Mr. CHAO [continuing]. Eligibility—when we are trying to calculate a payment, derive a payment, do data matches on the back end, that doesn't affect the Healthcare.gov operations.

Mr. GARDNER. How long will you have to test those parts that you are building?

Mr. CHAO. They are an ongoing basis. Depends on their build schedule.

Mr. GARDNER. So is it appropriate, given the performance of Healthcare.gov where we are at right now, to launch any new applications or features without testing them heavily before they go live?

Mr. CHAO. We are testing.

Mr. GARDNER. Mr. Chairman, I have several other questions and will follow up with you, but thank you for your time.

Mr. MURPHY. Thank you.

Now recognize Mr. Welch for 5 minutes.

Mr. WELCH. Thank you very much. Thank you for the hearing.

There is a mutual desire to get this thing to work, and there are really two models that we can use to deal with the failed rollout. One is to fix it, and the other is to use it as fodder to re-litigate the battle about whether health care is the law of the land. And my hope is that we are past that. There is an absolute urgency to make things work, and I know, Mr. Chao, that is your job, and I just want to put this into context. We had a big battle in this Congress, I was not here, over the passage of Medicare Part D. It was a largely partisan vote. The Republicans, under George Bush, were for it, most of the Democrats were against it, but it passed in a very close, tense vote. And my understanding is that as it then went into the implementation phase which required a computer program and a Web site, there were lots of significant difficulties with that program, and there were concerns about having it work.

And I just want to ask you a little bit about that history, so that we have a context for the challenges we have today, not at all as an excuse because there is real unity about needing to get this fixed, but are the actions we take about getting it fixed or about trying to derail and scuttle the overall healthcare program. America is going to have to judge.

But can you give us a sense what was going on inside the Agency when you were preparing the Medicare Part D Web site in 2005, and were there concerns and issues that needed to be addressed then?

Mr. CHAO. The biggest and most prominent example that I can recall was the concern around auto-assignment and auto-enrolling

Medicare—Medicaid full benefit dual eligibles to receive a Part D prescription drug benefit, and switching them over as of January 1, and that we had sent these enrollment files out to the plans—the health plans or Part D sponsors, around November, and in December it was some realization, you know, last-minute realization that pharmacists and pharmacies were—who were on the frontline of helping these beneficiaries, required, you know, some access to information to help them navigate this new change. So as an example, we scrambled and we developed a method for pharmacies to actually get access through authorizations to Medicare enrollment data for the dual eligibles that were enrolled so that, at point of sale, they can at least do things such as, you know, three day fills——

Mr. WELCH. Right.

Mr. CHAO [continuing]. Just to figure out what plan they might be in. And, you know, that is just an example. I recall that was a mass scramble, time crunch, had to get it in place, lots of, you know, working around the clock, lots of urgency, pushing many, many people, not just on the contractor and the staff side, but working with the prescription drug industry as a whole, including pharmacists, to make this happen.

Mr. WELCH. All right, and those problems continued even after the January 1 rollout date, my understanding.

Mr. CHAO. Correct, because it is not perfected. It is—it is not so much a technical issue, when you introduce a new business process, for example, in a procedure, you know, in an administrative aspect of health care, it takes a while for people to actually understand how that works, you know, as compared to learning the data system that is involved to support that business process. So it is more than just a technical issue.

Mr. WELCH. OK, and is it your view that, as we ultimately succeeded with Part D, we can ultimately succeed in terms of the technical Web site issues with Healthcare.gov?

Mr. CHAO. Certainly. I think it comes with being focused and driven to get at the root of the problem and to fix the systems, because on the technical issue side, it is solvable, very solvable, and we have shown that it has made improvements.

Mr. WELCH. OK, thank you very much.

I yield back.

Mr. MURPHY. Gentleman yields back.

Now recognize for 5 minutes the gentleman from Virginia, Mr. Griffith.

Mr. GRIFFITH. Thank you, Mr. Chairman.

Now, speaking of Medicare Part D, no one was required by law or force of penalty to subscribe to that, isn't that correct?

Mr. CHAO. No, but we did auto-assign, auto-enroll Medicare—Medicaid dual eligibles into Medicare Part D.

Mr. GRIFFITH. But it is a different animal than what we are dealing with now because a lot of Americans are being told they can't have their insurance so they are going to have to sign up through the Exchanges. So I do appreciate that, but there is a difference.

You know, one of the things that when you get time today to look at the report, and I think it is a symptom of the problems that this Web site has had, is that you were not included in the briefings

on the report that has come to light in the last 24 hours, but when you get a chance to read that, one of the things you will see is they thought there ought to be one person overseeing all of the different parts. And listening to the vendors who previously testified before this committee, it looked like they were each building their own part and then, in the last month, they had to squeeze it all together in the last two weeks, things were changing.

Another part of that report shows us that on a timeline, you really want to define your policy requirements prior to finishing the design and starting the build. Wouldn't you agree with that?

Mr. CHAO. That is the logical thing to do.

Mr. GRIFFITH. It is the logical thing to do, but in reality, we have heard testimony in this committee that they were changing policy, we know the big change on July the 2nd when all of a sudden the employer mandate was allegedly delayed—the President signed an executive order, I am not sure it has legal authority, but he did that, delayed that employer mandate. Further, we know from testimony that there were changes being made as close to the launch as 2 weeks before. So based on that, it would be the logical conclusion that you are going to have significant problems, wouldn't it?

Mr. CHAO. With the luxury of hindsight, I can see that, you know, there are contributors to the way the system performed when it was unveiled, but that is not——

Mr. GRIFFITH. Well, if you——

Mr. CHAO. But that is not, you know, I need to focus on fixing this thing.

Mr. GRIFFITH. And I know that is your focus is to fix it now, but also when you take a look at it, when you are still defining your policy requirements as late as two weeks prior to launch, it is very difficult to design and then to build and then to test a system and have it work, whether it is the security component or the performance component. It would be logical to do it in the proper order. When you do the illogical, you are liable to have problems. And I know you would agree with that, if you were free to answer honestly. And I would say to you that I also noticed that no one person was ever appointed to head this up while you were in charge of part of it, and you are in charge of making part of it work. It looks like there are at least six different representatives from different agencies that had a hand in overseeing what was going on, and no one had control over the others, isn't that correct?

Mr. CHAO. I think it was a governance committee that was formed.

Mr. GRIFFITH. A governance committee. And—isn't that interesting. And sometimes when you are trying to launch a big project like this though, you have to have one general in charge of the operation. Wouldn't that be logical?

Mr. CHAO. I would say that for the technical pieces, you know, I was responsible for making sure that the technical pieces were——

Mr. GRIFFITH. All right.

Mr. CHAO [continuing]. Organized.

Mr. GRIFFITH. And last month, this committee uncovered a September 27 memorandum indicating that Healthcare.gov launched without a full security control assessment. Administrator Tavenner

had to attest that she was aware that the launch carried security risks. Can you tell us what those risks are specifically?

Mr. CHAO. First of all, I think the incomplete testing—it was fully security tested through 3 rounds of testing so that when we—when Marilyn Tavenner signed the authority to operate on September 27, it had no high findings and had gone through the appropriate security tests.

Mr. GRIFFITH. So what she said was not accurate, that it had a—did not have a full security control assessment, she was mistaken when she testified in front of us on that?

Mr. CHAO. I think there is a part of that sentence that might be—it needs clarification. I think what we were trying to say was that the security control assessment was not tested for a full entire system of which we were still—remember, I—we are still building financial management aspects of it. I think it was just an acknowledgement that the—100 percent of the system was not complete at that time.

Mr. GRIFFITH. OK, and it is still not complete today, and the people of America want to know, you know, what is the security going to be——

Mr. CHAO. Well——

Mr. GRIFFITH [continuing]. If it is not completed on January 1.

Mr. CHAO. The October 1 pieces that were necessary, such as ensuring security privacy for those functions that I mentioned, were tested.

Mr. GRIFFITH. OK, and I appreciate that, but what can we expect on January 1?

I apologize, I yield back.

Mr. MURPHY. Thank you. And by the way, our prayers are with the family of State Senator Creigh in Virginia who is, I guess, in critical condition.

Mr. GRIFFITH. If I might——

Mr. MURPHY. Right.

Mr. GRIFFITH [continuing]. Take a—since you bring it up. If I might take a moment of personal privilege. I do appreciate your prayers. Creigh and I were in opposite parties, but just like on this committee, you form friendships. And he served with me in that Virginia House of Delegates before he went on to the Senate and went on to run for other offices. But he still is a sitting Senator, and it obviously has shaken everybody in Virginia. And he is a good man and our prayers are with him, and I encourage everybody to say a prayer for Senator Deeds and his family.

Mr. MURPHY. I thank the gentleman.

Now turning to Mr. Tonko for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair.

I would like to continue on that recent questioning of the document that my Republican colleagues have released.

Mr. Chao, this document was signed, I believe, on September 27, and it is an ATO, an authority to operate, memorandum to operate the Federally Facilitated Marketplace for 6 months, and implement a security mitigation plan.

Mr. CHAO. Correct.

Mr. TONKO. Can you tell us, are ATO's commonly used in Federal data systems?

Mr. CHAO. Yes. It is the, in essence, the last official sign-off to authorize a Federal system to go into operations.

Mr. TONKO. Thank you. And can you tell us why Administrator Tavenner signed this ATO rather than, well, perhaps other officials that might report to the administrator?

Mr. CHAO. I think the span of the stakeholders that were involved across the Agency has—we had not had a system that had this unprecedented involvement of so many different components, so that the recommendation by our chief information officer was to make a recommendation for the administrator to actually sign off on this, because she runs the entire agency.

Mr. TONKO. And the fact that she signed it is good news? It is an indication, I would believe, that officials at the highest level of CMS were briefed on and taking responsibility for site security?

Mr. CHAO. Correct, yes.

Mr. TONKO. Now, as I understand it, this document describes security testing for the Healthcare.gov Web site. It says that security testing of the marketplace was ongoing since inception and into September 2013. In fact, it says that, and I quote, "throughout the 3 rounds of security control assessment testing, all of the security controls have been tested on different versions of this system." Is that correct?

Mr. CHAO. Correct.

Mr. TONKO. But the document goes on to say that because of system readiness, a complete security assessment of all the security controls in one complete version of the system was not performed. It says that this lack of testing, and I quote, "exposed a level of uncertainty that could be deemed as a high risk."

Mr. CHAO. I didn't actually—I had recommended as part of that decision memo and I think at that time, as I mentioned earlier, you know, it is semantics, you know, not 100 percent of the system is built so you can't really consciously say you have it all available in one place to fully test, because not everything was needed for October 1. Only essential pieces involving Healthcare.gov were tested for security.

Mr. TONKO. So the document then indicated that CMS postponed a final security assessment screening, right, and the—in its place, CMS did put in place a number of mitigation measures. And it concluded that these measures would mitigate the security risks.

I want to take a moment to ask you about the September 27 ATO, and how the risks identified are being addressed. Can you describe their recommendations in that September 27 memo?

Mr. CHAO. You mean in terms of mitigations?

Mr. TONKO. Yes.

Mr. CHAO. OK, so on a daily basis, we run antivirus scans every 3 minutes, malware scans every 3 minutes, data full monitoring is a continuous effort, threat protection analysis against known bad IP's or hackers, I mentioned that in my opening remarks that it is continuous. On a weekly basis, we monitor operating system compliance, infrastructure system compliance, we conduct penetration testing, authenticated and unauthenticated, by marketplace security teams. We have a 24 by 7 security operations team. We conduct additional penetration testing, authenticated and unauthenticated, by another group of security professionals in CMS

that report under our chief of information security officer. We also conduct application software assurance testing, which is occurring biweekly. And on a monthly basis, we produce a plan of actions and milestones that keeps track and reports on any discovered weaknesses during all of this monitoring.

Mr. TONKO. So CMS is taking action that was recommended in the ATO?

Mr. CHAO. Correct.

Mr. TONKO. And do you have confidence in these and other measures you are taking to protect the security of Americans' personal information?

Mr. CHAO. I have high confidence.

Mr. TONKO. OK. As I understand it here, the remedial actions and the ongoing security testing are protecting the security of the Web site.

Mr. CHAO. Yes.

Mr. TONKO. And so perhaps the message coming from my Republican colleagues is that they do not want the Web site to work, and that they want to scare people from going on the Web site, when, in fact, we are hearing that security has been provided for.

Mr. CHAO. I think we have gone over and above, because we are very sensitive and we appreciate the nervousness around this new program with peoples' information.

Mr. TONKO. Well, we appreciate you building the security of the Web site, and responding to the actions recommended in the ATO memo.

Thank you so much. I yield back.

Mr. MURPHY. Thank you. Gentleman's time has expired.

Now recognize the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Chao, I spent 30 years in information technology as—I have been the chief information officer of publicly traded companies, as well as the director of the CIO staff at U.S. Special Operations Command, and I know the pressures that delivering on a system of this complexity, I know the pressures that are there.

I assume that you and I have a common goal here today, and that is to make sure that the American people hear the truth. Is that an accurate statement?

Mr. CHAO. That is correct.

Mr. JOHNSON. OK. Given that then, would it be OK if you and I have an understanding, because this is two IT guys talking to one another. If I ask you a question that you don't understand, would you ask me for clarification so that we can get to the bottom of it, because we want to dig down in here into some things that are pertinent?

Mr. CHAO. Yes, sir.

Mr. JOHNSON. OK, great. You know, under FISMA, agencies operating IT systems are required to establish security baselines, incorporate them into applications and networks, and test them to see that they are incorporated correctly. The use and review of this testing plan is typically known as a security control assessment. Several of the security control assessments for Healthcare.gov were either not completed or otherwise ignored.

So are you familiar with the four security control assessments that were completed on the various aspects of the Federally Facilitated Marketplaces?

Mr. CHAO. Not in intricate detail, but I think I—going back to what you said about ignored or missed, I think the most important thing to remember is that on September——

Mr. JOHNSON. Are you familiar with those security control assessments?

Mr. CHAO. I——

Mr. JOHNSON. Have you seen or read them?

Mr. CHAO. I have read the most important one, that is the one——

Mr. JOHNSON. Have you read all four of them?

Mr. CHAO. No, not all four.

Mr. JOHNSON. OK, could you turn to tab 4 of the document binder that you have in front of you? This is the security control assessment completed on October 11, 2013. Are you familiar with the findings of this security control assessment?

Mr. CHAO. Yes.

Mr. JOHNSON. OK. You testified a little earlier that it was your opinion, based on what you knew at the time, that the security control assessments—that security had been adequately addressed when Administrator Tavenner signed the document authorizing the operation of the Web site. Is that correct?

Mr. CHAO. Yes.

Mr. JOHNSON. But yet you just testified that you were not aware and you didn't read the security control assessment, so how can you make that assertion that security had been adequately addressed when you hadn't even read the control assessments yourself?

Mr. CHAO. I am thinking that there might be some mismatch in versions here. Yours says final report October 11 for Health Insurance Exchange August through September 2013, SCA report. I have the Federally Facilitated Marketplace decision security part——

Mr. JOHNSON. Well, I am talking about the one in your tab there.

VOICE. Excuse me, can we ask the witness to speak up a little bit? I am having difficulty hearing him.

Mr. CHAO. I am sorry.

Mr. JOHNSON. But I have got to move on because I don't have time to look through the binder.

Who develops the scope of a security control assessment before the contractor performs it?

Mr. CHAO. We have independent contractors that design our SCA testing.

Mr. JOHNSON. Do you need an application like the Data Services Hub or the Web site to be complete in order to test it for purposes of a security control assessment?

Mr. CHAO. I think that depends on, you know, we don't like testing security——

Mr. JOHNSON. Well, I can assure you that we don't.

Mr. CHAO. The—in terms of using live data, you know. So prior to going to production, we tend to conduct security——

Mr. JOHNSON. Well, let me ask you a question. Let us put up a slide. Are you familiar with the term sequel injection?

Mr. CHAO. Um-hum.

Mr. JOHNSON. OK. You know, sequel injection is a process that hackers use to gain access to sequel databases, relational databases, through a sequel. This is a screenshot directly off of Healthcare.gov that you see, if you put a semicolon in the search box, you get all of those different breakdowns of sequel injection.

Have—can you give me any idea how vigorous the testing was around sequel injection, and are you aware that potential hackers have the capability to go in through sequel injection and manipulate these strings?

Mr. CHAO. I can't speak to the exact—that situation. I think some of the folks that are coming up behind me in the other panel might be able to specifically address——

Mr. JOHNSON. I can assure you, Mr. Chairman, that I still have very serious concerns about the security aspects of this system.

And with that, I yield back.

Mr. MURPHY. Thank you. Gentleman's time has expired.

Now recognize Ms. Schakowsky for 5 minutes.

Ms. SCHAKOWSKY. I want to also focus on this particular system that the contractor, MITRE—I am here, Mr. Chao. Yes, OK.

Mr. CHAO. Sorry.

Ms. SCHAKOWSKY. We have heard this morning, we just heard, about the risks that the contract—contractor, MITRE, identified when it performed security control assessments for different components of Healthcare.gov. And at first glance, they can seem alarming, but my understanding is that all of these issues were mitigated for the functions on the Web site that launched on October 1. It is important to understand the general point of security testing, to identify any potential issues so they can be addressed before they became—become real problems. Asking MITRE to perform these assessments gives CMS and the contractors the opportunity to identify and resolve any security vulnerabilities before anyone's personal information could be put at risk.

So, Mr. Chao, does that sound to you like an accurate description? Do the security control assessments involve an iterative process where problems are identified and then mitigated?

Mr. CHAO. Yes, that is correctly characterized.

Ms. SCHAKOWSKY. So, Mr. Chao, I want to walk through some of these key security assessments to determine whether the high risks that MITRE identified have, in fact, been addressed.

In January and February of 2013, MITRE performed a security control assessment of EIDM, the account creation function on Healthcare.gov. According to the final report, MITRE identified several high-risk findings.

So, Mr. Chao, were these high-risk findings resolved and mitigated before the October 1 start of open enrollment in the Federal Marketplace?

Mr. CHAO. Yes, they were.

Ms. SCHAKOWSKY. And the fact is that they were noted in the—that fact is noted in the MITRE report.

OK, so MITRE also performed a security control assessment of the Data Services Hub in August 2013, and again identified several

high-risk findings. Were these findings resolved and also mitigated before the October 1 launch?

Mr. CHAO. Yes, and the Hub received authority to operate in August.

Ms. SCHAKOWSKY. Yes, and the fact is that was—and that fact was noted in the report.

I also want to discuss the security control assessment that MITRE performed over August and September 2013 for the Health Insurance Exchange. Mr. Chao, were all high risks identified in this assessment mitigated before October 1?

Mr. CHAO. Yes.

Ms. SCHAKOWSKY. I thank you. And what your answers confirm is that the system worked. MITRE identified potentially high risks—high security risks, and CMS made sure that they were mitigated before they would become major problems.

The MITRE reports do not show a flawed system, they show that CMS conducted security control assessments to identify problems, and then fixed those problems. And I hope that my Republican colleagues will keep these findings in mind when they talk about the security of Healthcare.gov. We don't want to alarm the public about security risks that have already been addressed by CMS and its contractors. It just seems to me that identifying risks that were named, it is important also to note that they were all fixed before the launch on October 1. And I thank you very much for your testimony.

I yield back.

Mr. CHAO. Thank you.

Mr. MURPHY. Gentlelady yields back.

And now I recognize the gentlewoman from North Carolina, Mrs. Ellmers, for 5 minutes.

Mrs. ELLMERS. Thank you, Mr. Chairman. And thank you, Mr. Chao, for being with us today.

Mr. Chao, I have a question about the subsidies, and some questions about some miscalculations that could be happening on the Exchange. Press reports have indicated that some subsidies are being miscalculated. In fact, one individual the President identified as a beneficiary of Obamacare now can't afford it. And, Mr. Chairman, I would ask unanimous consent to submit an article from CNN to the committee for the record.

[The information follows:]

November 19th, 2013
04:34 PM ET
Share this on:
Facebook
Twitter
Digg
del.icio.us
reddit
MySpace
StumbleUpon
13 hours ago

Bad news for woman cited as Obamacare success story

Posted by
CNN Senior White House Correspondent Jim Acosta

(CNN) - Jessica Sanford, the Washington State woman cited by President Barack Obama as an Obamacare success story, received more bad news Tuesday. Officials with the state's health exchange checked on her case and said she will not qualify for assistance in buying insurance.

Sanford had written the White House last month after purchasing what she thought was affordable health care coverage on the Washington state insurance exchange.

Part of her message was read by the President at a Rose Garden event at the a White House on October 21.

Woman cited by President as Obamacare success story frustrated by sign up process

But in the days that followed that presidential shout-out, Sanford received letters from Washington state's insurance exchange, notifying her she did not qualify for a tax credit she was originally told she would be getting.

After looking into Sanford's matter, officials with the exchange admit they made a mistake calculating her benefits, along with those for thousands of other Washington state residents.

"The Exchange would like to sincerely apologize to Jessica Sanford and all those affected in Washington State by this error," Washington Health Benefit Exchange CEO Richard Onizuka said in a statement provided to CNN.

"Unfortunately, Jessica Sanford is one of the individuals who is affected by this tax credit miscalculation," he added.

A 48 year old self-employed court reporter and single mother of a teenage son with ADHD, Sanford said it's now unlikely she will be able to afford to buy insurance.

"I'm not getting insurance unless I pay more money than I'm willing to pay," Sanford said.

"I've always been in this middle place. I make too much but I don't make enough."

Sanford said after her story appeared on CNN she was contacted by a person who identified herself as a spokeswoman in the White House press office.

Sanford said the White House official offered to help "in any way."

Asked about Sanford's story White House press secretary Jay Carney said the administration regrets the mix-up.

"We are certainly sorry as we can be that Jessica is one of the folks that has been affected by this," Carney said.

Sanford, an Obama and health care reform supporter, said "yes, I do" when asked if changes need to be made to the Affordable Care Act to help people like her.

Filed under: Healthcare • President Obama

Mrs. ELLMERS. OK. This is a single mom, has a teenage son with ADHD, went on the Washington State Exchange, had gotten an insurance quote for what she would pay at a gold price. Then she received notification that it was actually—the quote was actually higher for a silver plan. More confusion went on. Then even a cheaper plan at bronze level for $324. So, in other words, she ended up paying a lot more.

I guess in my questioning for you is, is this happening on the Healthcare.gov site or the Federal Marketplace?

Mr. CHAO. I think there are a lot of inputs to how an advanced premium tax credit is calculated. A person can come back and make some modifications to their income levels, to their household composition. So—and Washington is a State-based marketplace, so I can't really speak——

Mrs. ELLMERS. Um-hum.

Mr. CHAO [continuing]. For that particular case, but I think that Healthcare.gov allows people the flexibility to try several ways——

Mrs. ELLMERS. Um-hum.

Mr. CHAO [continuing]. To determine, you know, what their tax credit is.

Mrs. ELLMERS. OK, you know, and there again, I am just going based off the article. It doesn't seem to be that she had gone back to make any changes, it sounded to me like, you know, there were miscalculations that she was notified of. So again, my questioning is, is this happening in the Federal Exchange?

Mr. CHAO. I would need some specifics to be able to answer that.

Mrs. ELLMERS. OK.

Mr. CHAO. I think that if anyone ever does have issues with believing that their subsidies were incorrectly calculated, they could certainly call our call center to try to find out if it was correct or not.

Mrs. ELLMERS. So that is basically, you know, I am just asking how someone would address that, or how that would happen, if there were miscalculations then you could speak to someone personally and——

Mr. CHAO. Yes, we have both the call center and what we call an eligibility support work——

Mrs. ELLMERS. Um-hum. Do you know if this is what is happening?

Mr. CHAO. I——

Mrs. ELLMERS. Have you heard any reports of——

Mr. CHAO. I think there are many calls to the call center for many different reasons.

Mrs. ELLMERS. Um-hum.

Mr. CHAO. I don't know exactly, you know, I can't tell you there were 10 cases today or——

Mrs. ELLMERS. Um-hum, OK.

Mr. CHAO. But if you——

Mrs. ELLMERS. CGI—well, we can move on. I appreciate that. CGI, the contractor responsible for building Healthcare.gov, can you explain your role with them in the last weeks of September? Did you, you know, were you in contact with them, were you working with them one-on-one, were you in their office?

Mr. CHAO. Yes, I actually—I moved down to Herndon and lived in a hotel from September 10 to about the last week of October——

Mrs. ELLMERS. Um-hum.

Mr. CHAO [continuing]. And I worked at CGI almost every day.

Mrs. ELLMERS. So you were actually there in their offices, working out of their offices? OK.

Mr. CHAO. Yes.

Mrs. ELLMERS. One of the things that—I have got about a minute left on my time. The President announced a tech surge to fix the Web site. Who is involved in that surge?

Mr. CHAO. There—Todd Park is involved——

Mrs. ELLMERS. Um-hum.

Mr. CHAO [continuing]. And there are two fellows, one by the name of Mikey Dickerson, and another by the name of Greg Gershman.

Mrs. ELLMERS. Do you know about their compensation? How are they being compensated?

Mr. CHAO. I have no insight to that.

Mrs. ELLMERS. Um-hum. Do they have a contract or did they have to sign an agreement?

Mr. CHAO. I don't know.

Mrs. ELLMERS. Who do these individuals report to?

Mr. CHAO. I am not—actually, I am not sure who they have a contract with, or whether if they——

Mrs. ELLMERS. So—but you are in charge of the technical component to Healthcare.gov, and they don't report to you?

Mr. CHAO. No, they are part of a tech surge team that is being led by Jeff Zients.

Mrs. ELLMERS. OK.

Mr. CHAO. Right.

Mrs. ELLMERS. So Jeff Zients is really the person that they are reporting to?

Mr. CHAO. Right.

Mrs. ELLMERS. OK, thank you very much.

Mr. Chairman, my time has expired.

Mr. MURPHY. Gentlelady yields back.

Now go to Mr. Olson for 5 minutes.

Mr. OLSON. I thank the Chair. Welcome, Mr. Chao.

As you can imagine, sir, folks back home in Texas 22 have one simple question: Why, why, why did Healthcare.gov roll out on October 1 when most people in CMS, including yourself and every contractor writing codes and doing the testing, said stop, stop, stop, stop. We need more time. This Red Team document is frightening. I refer you to page 4 of the document, terms like limited end-to-end testing, parallel stacking of all phases. Stacking is vertical not parallel. Insufficient time and scope of end-to-end testing. Launch at full volume. And I refer you to a 7/16 email which you said you were worried that, and this is a quote, "crash the plane takeoff."

With all due respect, sir, it never got to the runway. It was still waiting at the ramp there, waiting for the pilots, the bags, the fuel, waiting for new tires. Using your analogy and my record as a naval aviator, Healthcare.gov was a "hangar queen," never ready to fly.

I do want to talk about—the folks back home I work for are most concerned about protection of their personal health information.

With so little testing, they are concerned about the lack of security control assessments, SCA's. And my question is, I will refer you to the document brief there, and on—please turn to tab 2, sir. My question concerns—you guys said that—this is a document you wrote for Ms. Tavenner, that you needed a 2-part mitigation plan. And part 2 is basically, you said, 1 of the recommended steps is to "conduct a full SCA test on the FFM in a stable environment where all security controls can be tested within 60 to 90 days of going live on October 1." The FFM will not be completed by November 30, so how can you conduct a full test of the SCA within 60 days of open enrollment? How could that happen when you are losing 30 days right off the bat?

Mr. CHAO. I think the 60 to 90 days refers to the inclusion of the final piece that needs to be built. What we mentioned earlier, which I just want to say that it is actually 30 percent of the systems are left to be developed, not 70 percent, and that 30 percent represents the payment aspect and the accounting aspects of making payments in the marketplace, for all marketplaces, not just for Federally Facilitated Marketplaces, and that that functionality has to be in place for the January 1 effective date enrollments. And so I think once we have that completed, we could do a full SCA across the entire system.

Mr. OLSON. But, sir, the document says October 1 rollout, 60 to 90 days after that. And apparently right now, we are going back to at least November 1 at the earliest for the rollout. I don't see how you get 60 days or 90 days of testing before we are going live again.

And one further question about the SCA's. How many SCA's did you identify and fix before the rollout on October 1, how many have been identified and fixed after rollout, and how many are still out there. What is the scope that my constituents should be worried about?

Mr. CHAO. The most important aspect is that there were no high findings in the SCA tests as of the October 1 rollout. And as I mentioned earlier, I read off a list of mitigation activities that we go over and above any system that we put into—we deploy and put in operations and monitor on a daily basis.

Mr. OLSON. When can you assure us that a full SCA will be conducted system-wide? Ever?

Mr. CHAO. When the last pieces of the system are completely built, which is not—you know, I don't want people to think that there hasn't been a full SCA. A full SCA has been conducted on the pieces that were needed for October 1 for eligibility enrollment. We have yet—we still have to build the financial management aspects of the system, which includes our accounting system and payment system and reconciliation system. Those will also have security testing involved as well.

Mr. OLSON. And the full end-to-end——

Mr. CHAO. Testing——

Mr. OLSON [continuing]. Testing, the whole, full system, when can we expect that to occur, sir? What date?

Mr. CHAO. I don't have an exact date, but it should be in—some time in December.

Mr. OLSON. So 2013, not 2014, 2015, 2016?

Mr. CHAO. Correct.

Mr. OLSON. 2013. OK, sir. One final question, and I want to refer back to your email from July 16 about needing to feel more confident about Healthcare.gov. I am assuming that some time in the last 4 months you got that confidence. What gave you that confidence? What was the trigger mechanism, when did that happen? Something changed in the last 4 months.

Mr. CHAO. I didn't say anything about having more confidence. I am always cautious, which is what I was trying to say earlier is that, until this is fixed, until the vast majority of people have a good experience going through here, and we have people who want to enroll, get enrolled, particularly for January 1, I am going to continue to focus on that along with the rest of the team. And, you know, and so it is not really about confidence level right now, it is about focusing on fixing the problem.

Mr. OLSON. And so we are not fine yet. The hangar queen is still at the hangar.

I yield back the balance of my time.

Mr. MURPHY. I thank the gentleman for yielding back.

What we are going to do is give each side 5 more total minutes, because Ms. DeGette has a couple of clarifying questions, I have a couple of clarifying questions. If anybody from my side needs some time, we will do that real quick.

Ms. DEGETTE.

Ms. DEGETTE. Thank you, Mr. Chairman.

Mr. Chao, I want to thank you for coming and spending the morning with us. I am going to try to be quick because I would like you to get back to wherever you are going and make this thing work. OK.

The first thing I want to clear up, because even though I thought we established it, my friends on the other side continued to ask you about this McKinsey document at tab 1, and I just want to clarify. You didn't—you weren't part of this Red Team evaluation, is that right?

Mr. CHAO. Correct.

Ms. DEGETTE. And you didn't really see this document until today, is that correct?

Mr. CHAO. Correct.

Ms. DEGETTE. So there were a lot of questions people asked you, hypothetical questions people asked you about this evaluation that you really don't know the answer to because you weren't involved in the process and you didn't see the document until today, right?

Mr. CHAO. Correct.

Ms. DEGETTE. Now, as I understand it, this evaluation was done in March/April 2013. Is that your understanding as well, this McKinsey evaluation?

Mr. CHAO. It is approximately that time.

Ms. DEGETTE. And do you have any knowledge of what that evaluation was supposed to be for? Was it a snapshot in time or do you even know?

Mr. CHAO. From the interviews that I had with McKinsey, it was about really 2 things. One was, I spent some time helping McKinsey understand the program.

Ms. DEGETTE. Uh-huh.

Mr. CHAO. Meaning how it worked, where we were in terms of status and schedule. I don't—I suppose it also includes a point in time kind of an assessment, because I educated them on exactly what was happening up to the date——

Ms. DEGETTE. Up to that time. Now, on page 4 of this assessment, I don't really want you to respond to this because you weren't involved in the document, but I do want to point out, there were a lot of questions that were asked today about the current situation, evolving requirements, multiple definitions of success, et cetera, but the people who were asking those questions today didn't talk about the last thing, which is in bold letters in a box, that says CMS has been working to mitigate challenges resulting from program characteristics. This was in March or April. And so without talking about this document necessarily, but I think what your testimony—what your job is really to identify issues throughout and try to mitigate them, is that right?

Mr. CHAO. Correct.

Ms. DEGETTE. And that is what you have tried to do throughout.

Mr. CHAO. It is a constant mitigation set of activities——

Ms. DEGETTE. And the administration has said it is going to try to have the Federal Exchange site working for 80 percent of the people by the end of November. Is that right? That is what we have been reading in the press.

Mr. CHAO. That is what the press quoted.

Ms. DEGETTE. OK.

Mr. CHAO. I think what we have been saying is the vast majority of——

Ms. DEGETTE. All right, and do you believe that that is a reasonable goal at this point?

Mr. CHAO. I think that is an attainable goal, given what I have seen so far.

Ms. DEGETTE. Do you think it is going to happen?

Mr. CHAO. I don't think there are any guarantees. I think we are still in a stage where we are trying to apply as much due diligence, acquiring additional assistance, the tech surge, looking at performance, fixing the functional defects, along with making sure that security monitoring is an ongoing basis. So I think there is still a lot of moving parts that it wouldn't be prudent to give 100 percent guarantees about where we are going to be at on an exact date——

Ms. DEGETTE. Well——

Mr. CHAO [continuing]. But I think we are on the right track.

Ms. DEGETTE. You are—OK, but what I will say to you is, truly, and you have heard this from all of us, all of us were disappointed that it didn't work on October 1. I am sure you were too.

Mr. CHAO. Very.

Ms. DEGETTE. And so we need this to be essentially working ASAP. For one thing, people who want insurance coverage as of January 1 have to sign up by December 15. So if it is not working for the vast majority of people by the end of November, that is going to be hard to do. Understood?

Mr. CHAO. We certainly understand that.

Ms. DEGETTE. OK. One last thing. Someone had asked you the question—or had made the assertion that 60 percent of the site was not working, but I am told that is not really accurate, that it

is really about 30 percent that is not working, and most of that is the backend which is the payment to insurance companies. So that is not necessarily the part that has to be working at this moment. Is that correct?

Mr. CHAO. Yes, it is not that it is not working, it is still being developed and tested.

Ms. DEGETTE. OK.

Mr. CHAO. Right.

Ms. DEGETTE. But that is the payment to the insurance companies.

Mr. CHAO. Correct.

Ms. DEGETTE. Right.

Mr. CHAO. Which involves testing with Treasury——

Ms. DEGETTE. OK.

Mr. CHAO [continuing]. And others.

Ms. DEGETTE. All right. Thanks, Mr. Chairman.

Mr. MURPHY. Thank you.

Recognize myself for 5 minutes.

Just let me follow up here that—then what you are saying this 30 percent is yet to develop on the payment end. On October 1, the day this went live, how much of the site was developed at that time?

Mr. CHAO. Probably—well 100 percent of all the priorities that were set for by the business for October 1, it was up and running.

Mr. MURPHY. OK, but what about the other parts?

Mr. CHAO. I think there was a reprioritization associated with, like, the shop employer, shop employee and the Spanish Web site that was——

Mr. MURPHY. But it was crashing for everybody. We have heard that it wasn't designed for that many people, it didn't pass a stress test, it never had end-to-end testing, and you are saying it was 100 percent ready?

Mr. CHAO. No, it——

Mr. MURPHY. I just want to make sure I understand. What——

Mr. CHAO. When I—it was 100 percent built, meaning——

Mr. MURPHY. One hundred percent built, but——

Mr. CHAO. Or the——

Mr. MURPHY [continuing]. Just not working.

Mr. CHAO. Yes, working functionally and——

Mr. MURPHY. Well, then it is not built.

Mr. CHAO [continuing]. Performing well, that——

Mr. MURPHY. If a car is built but you can't run the car, that car is not built. If a Web site isn't working, it is not built.

Mr. CHAO. Well, I am certainly not going to sit here and try to tell you that it was working well. So I do——

Mr. MURPHY. Yes, but you said on October 1 it was 100 percent built. I really need to know because you had said before you wish you had had more time, and you had just said to Ms. DeGette that your job was to identify issues and mitigate them. And since you would have liked to have had more time, and your job was to mitigate them, would you have liked to have seen this whole report from McKinsey that identified the problems so you didn't have to find them out?

Mr. CHAO. I don't—I—actually, I don't think it was necessary because I think this report was for—really for Marilyn Tavenner and others, and it was written for that level of consumption and that audience.

Mr. MURPHY. But you haven't seen this so you don't know. Or do you know?

Mr. CHAO. I am just assuming that that is why I wasn't——

Mr. MURPHY. OK, I just want you to stick with facts you know. So—well, what I am seeing here is from March on, Marianne Bowen, Jim Kerr, Todd Park, Brian Spivack, Michelle Snyder, Gary Cohen, Bill Corr, Mike Hash, Aryana Khalid, Katherine Sebelius, William Schultz, Michelle Snyder, Marilyn Tavenner, Mark Childress, Jeanne Lambrew and Ellen Montz all had briefings on this. Are those any people you work with?

Mr. CHAO. I have been in meetings with several of those folks.

Mr. MURPHY. Some of them. Since March and April?

Mr. CHAO. Yes.

Mr. MURPHY. And none of them raised any of these concerns to you, and you identified yourself that your job was to identify issues and mitigate them, but none of them identified——

Mr. CHAO. Within——

Mr. CHAO [continuing]. That, with all of these interviews and the 200 documents reviewed, that there were these problems?

Mr. CHAO. Within my day-to-day operational, you know, requirements to manage the contract, to manage schedule, to manage staff and——

Mr. MURPHY. Yes, but what you don't measure, you can't manage. And so I am concerned that this list of people who you work with were not communicating to you this document that you knew something existed because you, indeed, were interviewed on it yourself, but here we have this messy rollout that didn't work, that crashed, that only 6 people signed up the first day, and we still are concerned about problems, and yet it is puzzling to me why these key people just didn't talk to you about it. They gave you no hints that this existed?

Mr. CHAO. Perhaps that—I just was not included in certain discussions.

Mr. MURPHY. Well, if you knew then what you know now, would you have spoken up more with regard to rolling out this Web site on October 1?

Mr. CHAO. I wish I had the luxury of a time machine to go back and change things, but I can't do that.

Mr. MURPHY. I understand that, but it is a matter that—did you ask someone at that time for more time?

Mr. CHAO. No.

Mr. MURPHY. Why not?

Mr. CHAO. Because my direction——

Mr. MURPHY. From?

Mr. CHAO [continuing]. Was from Marilyn Tavenner, is to deliver a system on October 1.

Mr. MURPHY. So Marilyn Tavenner said deliver October 1. She had been in on these briefings from McKinsey that said there were serious problems. She was in at least 2 of them I believe. And this was at HHS Headquarters on April 4, she was there, and also at

the Eisenhower Executive Office Building on April 6. She was there, she was briefed on these problems. She said move it for October 1, and you, as the man who is in charge of making sure this works, she didn't tell you that those problems existed. Is that what you are saying today?

Mr. CHAO. I can't comment on that. I——

Mr. MURPHY. It is—well, it is either she told you or she didn't tell you. I am just curious.

Mr. CHAO. I don't think she told me in the context of this briefing. I think we have status meetings all the time in which we talk about ways to mitigate and to——

Mr. MURPHY. You—so you met with her frequently over those months, but she never brought up the extent of these concerns?

Mr. CHAO. Not the McKinsey report, no.

Mr. MURPHY. OK.

Mr. CHAO. I think we talked about certainly about issues and priorities for October 1.

Mr. MURPHY. I see.

Well, I have no further questions, so, Mr. Chao, I appreciate you spending so much time with us today. We are going to take a real quick 5-minute break. We recognize our next panel of witnesses has been sitting here for a while, so we will be right back in 5 minutes.

And thank you again, Mr. Chao.

Mr. CHAO. Thank you.

[Recess.]

Mr. MURPHY. All right, this hearing is reconvened.

I would now like to introduce the witnesses in the second panel for today's hearing, and thank you all for being so patient and waiting.

Our first witness is Jason Providakes. He is the Senior Vice President and General Manager for the Center for Connected Government at MITRE Corporation. He is also the Director of the Centers for Medicare and Medicaid Services Alliance to Modernize Medicare. Our second witness is Maggie Bauer. She is the Senior Vice President of Health Services at Creative Computing Solutions, Inc., also known as CCSi. She has extensive operations management experience in consulting, program management, IT infrastructure services, software development, lifecycle and end-user support on service-level drive performance-based programs. And our third witness is David Amsler. He is the Founder, President and Chief Information Officer at Foreground Security, Inc. He has more than 15 years of IT security experience, and he oversees the overall customer-centered vision and direction of Foreground Security, its industry-leading offerings and day-to-day operations.

I will now swear in the witnesses.

You are all aware that the committee is holding an investigative hearing, and when doing so, has the practice of taking testimony under oath. Do you have any objections to testifying under oath?

Ms. BAUER. No.

VOICES. No.

Mr. MURPHY. All the witnesses are in the negative there. The Chair then advises you that under the rules of the House and the rules of the committee, you are entitled to be advised by counsel.

Do any of you desire to be advised by counsel during your testimony today?

VOICES. No.

Mr. MURPHY. And all the witnesses have said no. In that case, would you please rise, raise your right hand and I will swear you in.

[Witnesses sworn.]

Mr. MURPHY. And all the witnesses responded, "I do."

You are now under oath and subject to the penalties set forth in Title XCIII, Section 1001 of the United States Code.

You may now give a 5-minute opening summary of your statement, Mr. Providakes.

STATEMENTS OF JASON PROVIDAKES, SENIOR VICE PRESIDENT, CENTER FOR CONNECTED GOVERNMENT, THE MITRE CORPORATION; MAGGIE BAUER, SENIOR VICE PRESIDENT, CREATIVE COMPUTING SOLUTIONS, INC.; AND DAVID AMSLER, PRESIDENT AND CHIEF INFORMATION OFFICER, FOREGROUND SECURITY, INC.

STATEMENT OF JASON PROVIDAKES

Mr. PROVIDAKES. Yes. All right, well, good morning, Chairman Murphy, and Ranking Member DeGette. My name is Jason Providakes, and I am here today on behalf of the MITRE Corporation. I serve as the director of the not-for-profit, Federally funded research and development center, operated by MITRE and sponsored by the U.S. Department of Health and Human Services.

The MITRE Corporation is chartered in the public interest to apply systems engineering skills and advanced technology, to address issues of critical national importance. We accomplish this through operation of research and development centers that support our Government sponsors with scientific research and development, analysis and systems engineering and integration as well.

Known as Federally funded research development centers, they are operated under a set of rules and constraints proscribed by the Federal acquisition regulations. The rules are designed to preserve the FFRDC's objectivity and dependence and freedom from conflict of interest.

MITRE operates FFRDC centers for seven Federal agency sponsors. We were awarded the contract to operate the CMS Alliance to Modernize Healthcare center about a year ago following a competitive bid. The center was charged with assisting CMS in modernizing its operation, and supporting the implementation of health reform, and the expansion of health care to millions of Americans.

MITRE serves as a technical, independent objective advisor to CMS. We have been supporting CMS successfully since about 2005 on a contract basis, prior to the establishment of the new center. We advise on health IT, helped plan and develop future policies, we provide technical evaluations and objective evaluation of business models, and assess new technology.

As part of its efforts to establish Healthcare.gov, CMS asked MITRE to conduct security assessments on parts of the site. And I appreciate the opportunity to clarify what our role was in assisting CMS on Healthcare.gov. We provide CMS with information se-

curity support and guidance under two contracts; the Office of Information Systems, and Enterprise Information Systems Group. Pursuant to tasks issued under those contracts, MITRE performed a total of 18 security control assessments, or SCA's, for components across the range of CMS enterprise systems. Most of these were performed on supporting infrastructure and development components. Six of the SCA's were directly related to Healthcare.gov, and were performed between September of 2012 and September of 2013.

MITRE performs various tasks as part of overall support for CMS enterprise security maintenance. A limited amount of that support is in the form of external penetration testing relative to CMS Web sites, including Healthcare.gov. MITRE is not in charge of security for Healthcare.gov. We were not asked nor did we perform end-to-end security testing. We have no view on the overall safety or security status of Healthcare.gov.

MITRE did not and does not recommend approval of—or disapproval of an authority to operate. Deciding whether and when to grant an ATO is inherently a governmental function that derives from the Government's assessment of overall risk posture. In this case, the Government made its ATO decisions based on a large set of inputs and factors, among which were 6 SCA's performed by MITRE. We do not have visibility into the many other factors that went into the Government's ATO decision. CMS did not advise MITRE whether or when ATO's were granted for the marketplace components being tested. In this case, the Government made its ATO decisions based on a large set of data.

Again, we were not asked to conduct end-to-end testing, rather we tested specific parts of Healthcare.gov, under a set of specific parameters established by CMS. We worked alongside the CMS-designated contractor in the course of testing to remediate risks as high, and in almost all cases, we succeeded. Our testing was accomplished in accordance with standard SCA engineering methodologies. In each case, we assessed component security control risks against CMS-defined security control parameters, on a high, moderate to low scale, and we recommended appropriate risk mitigations.

On site security control assessment, testing typically begins on a Monday and wraps up within a week. The tests against CMS-defined security control parameters, over the course of 5 days of testing, MITRE identifies the risk and assigns a remediation priorities for risks judged to be high and moderate levels. Security testing is designed to flush out and pinpoint the security weakness of a digital information system. This enables corrective remediations to be applied, and also allows the system operator to make necessary business judgments and tradeoffs about the overall system.

Because our role in performing the security control tests was limited in both time and scope, MITRE has no insight into how assessed security control risks were handled, or what other risks may have surfaced subsequent to the date of testing. Judgments about the potential impact of assessed security control risks on overall system operation or performance were business judgments made by CMS as part of the operating authority.

Through our broader partnership with the Federal Government, we remain committed to assisting CMS in working to enhance the care and delivery of health care for all Americans.

I would be happy to respond to your questions. Thank you.

[The prepared statement of Mr. Providakes follows:]

HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
STATEMENT OF THE MITRE CORPORATION
November 19, 2013

Good morning Chairman Murphy, Ranking Member DeGette and distinguished members of the committee. My name is Jason Providakes and I am here today on behalf of The MITRE Corporation. I serve as the director of the not for profit Federally Funded Research and Development Center (FFRDC), operated by MITRE and sponsored by the U.S. Department of Health and Human Services.

The MITRE Corporation is chartered in the public interest to apply systems engineering skills and advanced technology to address issues of critical national importance. We accomplish this through the operation of research and development centers that support our government sponsors with scientific research and development, analysis, and systems engineering and integration. Known as Federally Funded Research and Development Centers, they are operated under a set of rules and constraints prescribed by the Federal Acquisition Regulations (FAR). The rules are designed to preserve the FFRDC's objectivity, independence and freedom from conflict of interest.

MITRE operates FFRDC centers for seven federal agency sponsors. We were awarded the contract to operate the CMS Alliance to Modernize Healthcare center about a year ago, following a competitive bid process. The center is charged with assisting CMS in modernizing its operations and supporting the implementation of health reform and expansion of health care to millions of Americans.

MITRE serves as a technical independent, objective advisor to CMS/HHS. We have been supporting CMS/HHS successfully since 2005 on a contract basis prior to the establishment of the new center. We advise on Health IT; help plan and develop future policies; provide technical evaluation and objective evaluation of business models; and assess new technology.

As part of its efforts to establish HealthCare.gov, CMS asked MITRE to conduct security assessments on parts of the site. I appreciate this opportunity to clarify what our role was in assisting CMS on HealthCare.gov.

We provide CMS with information security support and guidance under two contracts with the Office of Information Systems (OIS), Enterprise Information Security Group (EISG). Pursuant to tasking issued under those contracts, MITRE performed a total of 18 Security Control Assessments, or SCAs, for components across a range of CMS enterprise systems. Most of these were performed on supporting infrastructure (utilities) and development components. Six of the SCAs were directly related to HealthCare.gov and were performed between September 17, 2012 and September 20, 2013.

MITRE performs various tasks as part of our overall support for CMS enterprise security maintenance. A limited amount of that support is in the form of external penetration testing relative to CMS websites including HealthCare.gov.

MITRE is not in charge of security for HealthCare.gov. We were not asked, nor did we perform "end-to-end" security testing. We have no view on the overall "safety" or security status of HealthCare.gov.

MITRE did not and does not recommend approval or disapproval of an Authority to Operate (ATO). Deciding whether and when to grant an ATO is an inherently governmental function which derives from the government's assessment of overall risk posture. In this case, the government made its ATO decisions based on a large set of inputs and factors, among which were the six SCAs performed by MITRE. We do not have visibility into the many other factors that went into the government's ATO decision. CMS did not advise MITRE whether or when ATOs were granted for the Marketplace components tested. In this case, the government made its ATO decisions based on a large set of data.

Again, we were not asked to conduct end-to-end testing. Rather, we tested specific parts of HealthCare.gov within specific parameters established by CMS. We worked alongside the CMS-designated contractor in the course of testing to remediate risks assessed as "high," and in almost all cases we succeeded.

Our testing was accomplished in accordance with standard SCA engineering methodologies. In each case, we assessed component security control risks against CMS-defined security control parameters on a high-moderate-low scale, and we recommended appropriate risk mitigations. On-site Security Control Assessment testing typically begins on a Monday and wraps up within the week. It tests against CMS defined security control parameters. Over the course of the five days of testing, MITRE identifies risks and assigns remediation priorities for risks judged to be at high and moderate levels.

At the committee's request, we previously made available to committee staff the final reports of the six Security Control Assessments relevant to HealthCare.gov. Security testing is designed to flush out and pinpoint the security weaknesses of a digital information system. This enables corrective remediations to be applied and also allows the system operator to make the necessary business judgments and tradeoffs about the overall system.

By definition and design, Security Control Assessment reports will typically contain data that, in the hands of a malicious actor, could be used to compromise the security and privacy of information stored on the affected site. It was, of course, no different in the case of the SCAs performed on HealthCare.gov components. We accordingly redacted from our delivered documents portions that essentially could serve as a technical roadmap to a hacker bent on causing harm.

We also would like the committee to understand and appreciate that, even with the redactions, the information contained in the delivered materials could pose a significant risk to the confidentiality of consumer information accessible through HealthCare.gov.

Because our role in performing the security control tests was limited in both time and scope, MITRE has no insight into how assessed security control risks were handled or what other risks may have surfaced subsequent to the date of testing. Judgments about the potential impact of assessed security control risks on overall system operations or performance were business judgments made by CMS as the operating authority.

Through our broader partnership with the federal government, we remain committed to assisting CMS in working to enhance the care and delivery of health care for all Americans.

I would be happy to respond to your questions. Thank you.

Mr. MURPHY. Thank you.

Now turn to Ms. Bauer for her opening statement.

STATEMENT OF MAGGIE BAUER

Ms. BAUER. Good afternoon, Chairman Murphy, Ranking Member DeGette. My name is Maggie Bauer, and I am a Senior Vice President at Creative Computing Solutions, Inc., CCSi.

I have responsibility for CCSi's Federal health contracts, including the Centers for Medicare and Medicaid Services, Veterans Affairs, the Department of Health and Human Services National Institutes of Health, and the Military Health Service.

In addition to health-related services, CCSi delivers program and project management services, cyber security services and enterprise systems engineering, exclusively to the Federal Government.

CCSi was founded in 1992 by Dr. Manju Bewtra.

In August of 2012, CMS awarded CCSi a contract to provide security oversight of the CMS e-cloud. The e-cloud refers to CMS's virtual data center, which hosts systems and applications that support the Affordable Care Act. Foreground Security is their subcontractor, and we function as a fully integrated team.

CCSi's role on this contract is to provide security operations monitoring and management, including 24 by 7 by 365 security monitoring from a secure operation center, otherwise known as a SOC. We monitor the perimeter firewalls and network devices for the e-cloud, and we scan applications for security incidents. These scans do not measure or track availability, up/downtimes or latency. If we detect an anomaly, we follow the CMS-approved incident response plan procedures for identified security incidents, such as network security configuration flaws or vulnerabilities in the network, security devices or in applications. CCSi's contract does not extend to remediating security incidents.

CCSi's scope of work includes configuration, tuning, monitoring and management of CMS Government-furnished equipment that resides in the Verizon Terremark security monitoring zone. We review log files, we conduct event analysis, we provide reporting on security incidents, all of this under the direction and supervision of CMS.

Activities involving the development, scaling, testing, release or administration of the Federal Exchange Program, Healthcare.gov, the Federal Exchange, or the Federally Facilitated Marketplace are not within the scope of our contract.

I would be pleased to answer any questions that you have. Thank you.

[The prepared statement of Ms. Bauer follows:]

Written Testimony of:

Maggie Bauer
Senior Vice President
Creative Computing Solutions, Inc. (CCSi)

Prepared for:
The House Committee on Energy and Commerce
November 19, 2013

Good morning Chairman Upton, Ranking Member Waxman and distinguished members of the Committee. My name is Maggie Bauer and I am a Senior Vice President at Creative Computing Solutions, Inc. (CCSi). I have responsibility for CCSi's federal health contracts, including: Centers for Medicare and Medicaid Services (CMS); Veterans Affairs (VA); the Department of Health and Human Services (HHS) National Institutes of Health (NIH) and the Military Health Service (MHS). In addition to health-related services, we deliver program and project management services, cyber security services, and enterprise systems engineering exclusively to the federal government. CCSi was founded in 1992 by Dr. Manju Bewtra.

In August of 2012, CMS awarded CCSi a contract to provide security oversight of the CMS eCloud. The eCloud refers to CMS's virtual data center which hosts systems and applications that support the Affordable Care Act. CCSi was competitively awarded this contract in August 2012 under the Alliant Small Business (SB) Government-wide Acquisition Contract (Alliant SB GWAC) which is a Multiple Award, Indefinite Delivery, Indefinite Quantity (IDIQ) contract vehicle. Foreground Security Services (FGS) is our subcontractor on this contract. Together, we are an integrated team of 22 staff members, 6 of whom are CCSi employees and 16 of whom work for FGS.

CCSi's role on this contract is to provide security operations monitoring and management including 24x7x365 security monitoring from a Security Operations Center (SOC). We monitor the perimeter firewalls and network devices for the eCloud and we scan applications for vulnerabilities. These scans do not measure or track availability, up/down times or latency. If we detect an anomaly, we follow the CMS approved Incident Response Plan (IRP) procedures for identified network security configuration flaws and vulnerabilities in network and security devices and in applications. CCSi's contract does not extend to remediating any security configuration flaws or vulnerabilities in the network infrastructure nor does it include remediation of any vulnerability discovered in applications.

CCSi's scope of work also includes configuration, tuning, monitoring and management of CMS government furnished equipment (GFE) that resides in the Terremark security monitoring zone. We review log files, conduct event analysis, and provide reporting on security incidents under the direction and supervision of CMS.

Examples of the functions that CCSi performs under this contract include:

- Detecting malicious activity, preventing unauthorized access to systems, and recommending threat protections

- Maintaining, patching operating and tuning CMS security appliances, tools and services to prevent and detect intrusions
- Ensuring that systems are configured for routine scans and import scan results into security monitoring tools to assess system risk
- Maintaining baseline configuration of the information system and monitor for unexpected changes to the baseline
- Planning and supporting integration of security components of existing tools

Activities involving the development, scaling, testing, release or administration of the Federal Exchange Program System, "healthcare.gov," the "Federal Exchange" or the Federally Facilitated Marketplace or "FFM" are not within scope of our contract.

I would be pleased to answer any questions that you have. Thank you.

Mr. MURPHY. Thank you, Ms. Bauer.
Mr. Amsler, you are recognized for 5 minutes.

STATEMENT OF DAVID AMSLER

Mr. AMSLER. Thank you, sir.

Chairman Murphy, Ranking Member DeGette, members of the subcommittee, good afternoon and thank you for inviting me to testify at this hearing on the security of the Web site, Healthcare.gov.

I am the president and chief information officer of Foreground Security. I also founded the company. We provide cyber security consulting, training and services for both private-sector and Government agencies. Our clients include Fortune 100 companies, smaller but highly targeted firms, and Government agencies.

We defend our customers against an increasingly intricate threat and threat actors, through an integrated approach that entails building security architecture and assessing, monitoring and responding to attacks against our customer environments.

Foreground Security is a small but growing dedicated cyber security business located in Herndon, Virginia, and Florida. Our roughly 100 employees are highly trained and committed to serving our clients.

Foreground Security is one of the companies hired to help develop a robust operational security management program for the new virtual data center created to implement the Affordable Care Act. We are subcontracted to our teammate, Creative Computing Solutions, Inc., or CCSi, which is the prime contractor for the Centers for Medicare and Medicaid Services.

Our role with CCSi includes a number of objectives relating to the security environment of Healthcare.gov. I think of our role as encompassing 3 phases. First is the creation of the security monitoring environment. This entailed getting key staff in place, identifying needed security monitoring software and hardware, and building out a dedicated security operation center, or SOC, from which all monitoring is performed. Second is building those security monitoring capabilities identified in phase 1 into the cloud environment itself. This has been the most challenging part of our contract, in large part because we have had to construct security monitoring capabilities while the system itself is being built. Our work on this phase continues. And third is actually monitoring the environment, which itself can be thought of as having two components. One is day-to-day, continuously searching for malicious activities including reporting and defending against them when they do occur. The other is monitoring known malicious actors or groups in advance of attacks to proactively identify the techniques or tactics they may be using or planning to use to compromise this environment. These are our main and State responsibilities relating to the security environment.

We have worked very closely with CMS and Verizon Terremark on all phases of our work. CMS reviews and approves any capability we place in the environment, and Verizon Terremark, as the host of the environment, helps determine what security measures are placed in the virtual data center.

Prospective on our role is important. While our work for CMS is essential, it is narrowly focused, and we were not involved in the

design of the site, developing the software that runs it, or its administration. To that end, we do not monitor the site for performance purposes. Foreground Security is just 1 member of the security team, in addition to the other companies represented today here on this panel, Verizon Terremark, URS, CGI and QSSI, all play key roles in developing and testing the security of Healthcare.gov.

I am proud of the work that Foreground Security has undertaken and continues to undertake in order to allow families and individuals looking for health insurance to use the Healthcare.gov Web site, secure in the knowledge that their personal information is being protected with state-of-the-art monitoring and defenses. To this point, Foreground Security has fulfilled its obligations to CMS on time and under budget. We are dedicated to secure the operation of Healthcare.gov, and take extremely serious the obligations to the public trust.

I welcome any questions you may have.

[The prepared statement of Mr. Amsler follows:]

Testimony of David Amsler
President and Chief Information Officer
Foreground Security, Inc.

Hearing before the House Energy & Commerce Committee
Subcommittee on Oversight and Investigations
"Security of HealthCare.gov"
November 19, 2013

Chairman Murphy, Ranking Member DeGette, members of the Subcommittee, good afternoon and thank you for inviting me to testify at this hearing on the security of the web site, HealthCare.gov. I am the President and Chief Information Officer of Foreground Security, Inc. I also founded the company, which provides cyber-security consulting, training and services for both private sector and government entities. Our clients include Fortune 100 companies, smaller but highly-targeted firms, and government agencies. We defend our customers against increasingly intricate threats and threat actors through an integrated approach that entails building security architecture and assessing, monitoring, and responding to attacks against our customer environments.

Foreground Security is a small but growing, dedicated cyber-security business located in Herndon, Virginia and Florida. Our roughly 100 employees are highly-trained and committed to serving our clients.

Foreground Security is one of the companies hired to help develop a robust operational security management program for the new virtual data center created to implement the Affordable Care Act. We are a subcontractor to our teammate, Creative Computing Solutions, Inc.—or "CCSI"—which is the prime contractor for the Centers for Medicare and Medicaid Services ("CMS").

Our role with CCSI includes a number of objectives relating to the security environment of HealthCare.gov. I think of our role as encompassing three phases. First, is the creation of the security monitoring environment. This entailed getting key staff in place, identifying needed security monitoring software and hardware, and building out a dedicated securities operations center, or "SOC", from which all monitoring is performed.

Second, is building those security monitoring capabilities identified in phase one into the cloud environment itself. This has been the most challenging part of our contract, in large part because we have had to construct security monitoring capabilities while the system itself is being built. Our work on this phase continues.

And third, is actually monitoring the environment, which itself can be thought of as having two components. One is day-to-day, continuous searching for malicious activities, including reporting and defending against them when they occur. The other is monitoring known, malicious actors or groups in advance of

attacks to proactively identify techniques or tactics they may be using or planning to use to compromise this environment. These are our main, end-state responsibilities relating to the security environment.

We have worked very closely with CMS and Verizon/Terremark on all phases of our work. CMS reviews and approves any capability we place in the environment and Verizon/Terremark, as the host of the environment, helps determine what security measures are placed in the virtual data center.

Perspective on our role is important. While our work for CMS is essential, it is also narrowly focused, and we were not involved in the design of the site, developing the software that runs it, or its administration. To that end, we do not monitor the site for performance purposes. Foreground Security is just one member of the security team. In addition to the other companies represented today on this panel, Verizon/Terremark, URS, CGI, and QSSI all play key roles in developing and testing the security of HealthCare.gov.

I am proud of the work that Foreground Security has undertaken—and continues to undertake—in order to allow families and individuals looking for health insurance to use the HealthCare.gov site, secure in the knowledge that their personal information is being protected with state-of-the art monitoring and defenses. To this point, Foreground Security has fulfilled its obligations to CMS

on time and under budget. We are dedicated to the secure operation of HealthCare.gov and take extremely seriously our obligations to the public trust.

I welcome any questions you may have.

Mr. MURPHY. Thank you, Mr. Amsler.

Couple of questions I want to begin with. First of all, I will start with you, Mr. Amsler. You were here throughout Mr. Chao's testimony, all three of you were. Do you have any concerns about any comments that were made by Mr. Chao?

Mr. AMSLER. I wouldn't have any specific concerns——

Mr. MURPHY. Ms. Bauer?

Mr. AMSLER [continuing]. I would like to voice.

Ms. BAUER. No.

Mr. MURPHY. Mr. Providakes?

Mr. PROVIDAKES. No concerns.

Mr. MURPHY. All right. Mr. Amsler, you had said that in addition to the other companies represented today in this panel, Verizon Terremark, URS, CGI and QSSI, all played key roles in developing and testing the security of Healthcare.gov. Are you also referring to Ms. Bauer's company played a role in this?

Mr. AMSLER. I view them as our teammate, I view them as one of us.

Mr. MURPHY. Because I thought in her testimony she said that they were not that involved. So let me ask you, with this many companies involved, who did you all report to?

Mr. AMSLER. Well, our customer was CMS, and the security team——

Mr. MURPHY. Person. Is there a person?

Mr. AMSLER. Our direct Government technical lead, his name is Tom Shankweiler.

Mr. MURPHY. And with regard to this, with all of these companies involved playing key roles in developing and testing security, is that typical to have so many companies involved as opposed to one that is trying to do the end-to-end work on this?

Mr. AMSLER. Well, we have experienced all sizes of implementations. This one is obviously, certainly one of the largest that I have ever seen undertaken. I have certainly seen lots of people involved, but probably not this many.

Mr. MURPHY. Mr. Providakes, is this typical to have so many companies involved in dealing with the security in a site?

Mr. PROVIDAKES. Not really number of companies that were involved, but having two or three is not untypical to have on the complexity of a site like this.

Mr. MURPHY. I just wondered if that added to the complexity of trying to monitor security of the site.

Mr. PROVIDAKES. If it is well-managed from a program perspective——

Mr. MURPHY. Was it well-managed?

Mr. PROVIDAKES. I would not know.

Mr. MURPHY. From your perspective?

Mr. PROVIDAKES. I don't—we weren't involved in that level of insight on that. I believe, you know——

Mr. MURPHY. All right, Ms. Bauer, were you involved in that level, and was it well-managed from your point of view?

Ms. BAUER. Our management from CMS has been on a very regular basis. We have daily meetings, in fact, since Healthcare.gov went live. Those meetings actually began, or ramped up I should

say, to hourly and then back to way to about every 4 hours, and now they are on a shift basis of three times a day.

Mr. MURPHY. Well, you just said activities involving the development, scaling, testing, release or administration of the Federal Exchange Program system, Healthcare.gov, the Federal Exchange or the Federally Facilitated Marketplace, or FFM, are not within the scope of your contract. So you were not involved in the security issues involved with those Web sites?

Ms. BAUER. The security, yes, but not the development, scaling, or testing of the Healthcare.gov applications, per se.

Mr. MURPHY. Were you involved with the testing of the security?

Ms. BAUER. Yes.

Mr. MURPHY. And was it working?

Ms. BAUER. Yes.

Mr. MURPHY. At October 1?

Ms. BAUER. Everything that was under our scope.

Mr. MURPHY. Under your scope.

Ms. BAUER. Yes——

Mr. MURPHY. But in terms of——

Ms. BAUER [continuing]. Was functioning.

Mr. MURPHY [continuing]. How it relates to other parts, you don't know?

Ms. BAUER. I would not know that.

Mr. MURPHY. OK. Mr. Amsler, how about for you, were your parts working OK in your individual part, and was that also tested with regard to the others?

Mr. AMSLER. Congressman, to be clear, as far as our work is concerned, our focus worked around operational monitoring security and some testing, we absolutely were working. I can't speak to the rest of the groups and the teams that were involved in development, or even the SCA——

Mr. MURPHY. What I am trying to find out, was that——

Mr. AMSLER [continuing]. People who were not involved.

Mr. MURPHY [continuing]. Typical, atypical, and would you be concerned about how your parts worked in conjunction with the site overall, or is that not typically a question you would ask? Well, it is like this: If you design a part for a car and you know your part is working, would you like to know if the car works?

Mr. AMSLER. Absolutely.

Mr. MURPHY. And so that is what I am asking all of you, would you have liked to have known that if your segments may have worked on their own, but you didn't know whether or not it worked at the whole system security. Is that correct, Mr. Providakes?

Mr. PROVIDAKES. Well, that would be correct.

Mr. MURPHY. Ms. Bauer?

Ms. BAUER. Yes.

Mr. MURPHY. OK. Mr. Providakes, CMS adopted the security controls you developed, correct?

Mr. PROVIDAKES. That is correct.

Mr. MURPHY. And are these controls embedded in the applications at the direction of CMS?

Mr. PROVIDAKES. They were assessed, but yes, they were embedded for the configuration changes would be made based on the configuration controls.

Mr. MURPHY. And at what point of the application development phase should security controls begin to be embedded into the application?

Mr. PROVIDAKES. Well, at the production phase. Generally, when we test with an SCA, we are assuming that we are looking at the production-ready version of the application, and then we apply those CMS security controls we talked about and assess those against the production-ready version of that application.

Mr. MURPHY. Are they embedded into the architecture of Healthcare.gov?

Mr. PROVIDAKES. The overall CMS enterprise security controls are to be applied across all the systems of Healthcare.gov.

Mr. MURPHY. So they should be embedded then into Healthcare.gov?

Mr. PROVIDAKES. It should be.

Mr. MURPHY. Were they?

Mr. PROVIDAKES. I have no way of knowing that.

Mr. MURPHY. Ms. Bauer, do you know if they were?

Ms. BAUER. I do not know.

Mr. MURPHY. Mr. Amsler?

Mr. AMSLER. I wouldn't know the answer to that.

Mr. MURPHY. OK. But you all worked on these security parts. We don't know if they were embedded and you don't know if anybody did testing, but you would have liked to have seen that. Am I correct with all of you?

Mr. PROVIDAKES. No, just parts. Just some parts.

Mr. MURPHY. Ms. Bauer, correct?

Ms. BAUER. Correct

Mr. MURPHY. Mr. Amsler?

Mr. AMSLER. Correct.

Mr. MURPHY. Thank you.

And now I will yield to Ms. DeGette for 5 minutes.

Ms. DEGETTE. Thank you, Mr. Chairman.

As Mr. Chao testified, it is part of CMS's protocols that they hire independent contractors to test different parts of the security aspects of the site. Is that your understanding as well, Mr. Providakes?

Mr. PROVIDAKES. Yes, it is.

Ms. DEGETTE. And is it yours, Ms. Bauer?

Ms. BAUER. Yes.

Ms. DEGETTE. And is it yours, Mr. Amsler?

Mr. AMSLER. Yes.

Ms. DEGETTE. So, Mr. Providakes, I want to ask you first. You testified your company was not hired to perform end-to-end security testing, is that correct?

Mr. PROVIDAKES. That is correct.

Ms. DEGETTE. And so what your job was to assess and identify risks and specific components of Healthcare.gov, to work with CMS and to address those concerns and report on the findings and results. Is that correct?

Mr. PROVIDAKES. That is correct.

Ms. DEGETTE. And am I correct that in virtually all cases, when you did identify high risks in Healthcare.gov components, CMS was able to mitigate those risks before the system went live?

Mr. PROVIDAKES. Yes. Almost all the high risks were mitigated.

Ms. DEGETTE. And you said in your testimony—in your written testimony, MITRE is not in charge of security for Healthcare.gov. We were not asked, nor did we perform, end-to-end security testing. We have no view of the overall safety or security status of Healthcare.gov. That is because you were only asked to do a narrow assessment of part of it, right?

Mr. PROVIDAKES. A narrow assessment in scope and in a time that is——

Ms. DEGETTE. In time.

Mr. PROVIDAKES. In time.

Ms. DEGETTE. Now, I just want to ask you, what is your personal view of the overall safety or security of Healthcare.gov, having worked on this, at least some aspects of it?

Mr. PROVIDAKES. Well, my personal perspective——

Ms. DEGETTE. Uh-huh.

Mr. PROVIDAKES [continuing]. Knowing CMS experience in the past, as Henry Chao alluded to, they do a very solid job in terms of securing their systems—

Ms. DEGETTE. And——

Mr. PROVIDAKES [continuing]. Historically.

Ms. DEGETTE. And what you were doing was part of the same types of things CMS has done to secure their systems in the past——

Mr. PROVIDAKES. That is correct.

Ms. DEGETTE [continuing]. Is that right?

Mr. PROVIDAKES. That is correct.

Ms. DEGETTE. Ms. Bauer—now, as I understand it, Mr. Amsler, your company works sort of as a subcontractor of Ms. Bauer's company. Is that right?

Mr. AMSLER. Yes.

Ms. DEGETTE. OK. So what you folks do is your company—CCSi monitors the firewalls and network devices for the e-cloud that hosts Healthcare.gov, and scans the Web site's application for security vulnerabilities. Is that correct?

Ms. BAUER. That is correct.

Ms. DEGETTE. And on October 22, you briefed this committee, and I want to ask you, at that time, had you detected any activity that you would consider to be out of the ordinary for a system like this?

Ms. BAUER. Not out of the ordinary, no.

Ms. DEGETTE. OK. And are you continuing to monitor the Web site moving forward?

Ms. BAUER. Yes, we continue to perform all the functions of our contract.

Ms. DEGETTE. And why is that?

Ms. BAUER. I am sorry?

Ms. DEGETTE. Why are you continuing to monitor the functions?

Ms. BAUER. Because that is the scope of our contract, is to continually——

Ms. DEGETTE. OK. And have you——

Ms. BAUER [continuing]. Monitor it.

Ms. DEGETTE. Have you detected any activity since October 22 that you considered to be out of the ordinary?

Ms. BAUER. We would detect activity on a daily, if not hourly basis. That is part of the nature of security monitoring. Whether it is extreme or out of the ordinary, there is nothing that has been brought to my attention that would——

Ms. DEGETTE. And would that be then reported to CMS?

Ms. BAUER. Yes, there is an incident response plan, and we follow the procedures of that plan.

Ms. DEGETTE. And have you seen anything that would indicate some terrible problem with the Web site vis-a-vis security?

Ms. BAUER. Nothing that I have seen or that has been escalated to me, no.

Ms. DEGETTE. OK. And there is another contractor as I understand that has also been asked to look at other aspects, and that is Verizon. They are not here today. Is that your understanding as well?

Ms. BAUER. Yes. Yes.

Ms. DEGETTE. So Ms. Bauer, has your company worked with CMS before? Mr. Providakes said his has on security issues.

Ms. BAUER. No, we have not, but we——

Ms. DEGETTE. OK.

Ms. BAUER [continuing]. Have other security work.

Ms. DEGETTE. OK. And Mr. Amsler, what about your company?

Mr. AMSLER. Not directly for CMS——

Ms. DEGETTE. OK.

Mr. AMSLER [continuing]. But other HHS——

Ms. DEGETTE. OK, so you wouldn't know whether this is—kind of mirrors other security activity with CMS. But, Mr. Providakes, you are telling me that, with what your company has done before, you are seeing a similar concern and readiness for security applications?

Mr. PROVIDAKES. Well, what I said was that following CMS's approach towards security, they do execute, you know, 10, 20, 70 SCA's a year that we actually executed for CMS. So part of their process is, before they execute an ATO, they look for the input of these SCA's, which is a very rigorous process, a definition, defined in a parameter in a moment of time that we would conduct these SCA's for CMS as input to the ATO process.

Ms. DEGETTE. Right. OK, thank you.

Thanks, Mr. Chairman. I appreciate it.

Mr. MURPHY. Let me ask clarification of something Ms. DeGette said.

Mr. PROVIDAKES. Sure.

Mr. MURPHY. She asked you a question about CMS and their work on this, and you used the word historically. Were you referring then to the Healthcare.gov Web site or in the past they were?

Mr. PROVIDAKES. No. In the past. Broadly across CMS in terms of their security rigor that they apply across their systems.

Mr. MURPHY. Thank you.

Mr. Olson, you are recognized for 5 minutes.

Mr. OLSON. I thank the Chair. I mostly want to thank the witnesses for your patience being here. It has been a long day, I know that.

Very brief questions. I mean, getting Healthcare.gov up and running is not rocket science, and that is good because if it were, we would still be waiting to land on the moon over 50 years later.

You may have seen the McKinsey report, the Red Team report. Have you all seen that?

Ms. BAUER. I have not.

Mr. OLSON. OK. I will get the copies to you. I just want to ask some questions about the report. And I apologize that you haven't seen it, but it compares on page 4 ideal, large-scale programs and the current state of Healthcare.gov. And I want to—just some yes-or-no questions, do you agree with the statements from this report. And again, it is compared to large-scale program development ideal program with the characteristics of Healthcare.gov. The first ideal situation, clear articulation of requirements and success metrics in Healthcare.gov, evolving requirements and multiple definitions of success. Do you agree with those assessments that that is ideal, and that is what has happened with Healthcare.gov, Mr. Providakes? Yes or no, sir? Don't want to put you on the spot.

Mr. PROVIDAKES. It is very difficult to answer that question. Is that a hypothetical question in terms of——

Mr. OLSON. Hypothetical, yes, sir. I mean the ideal program is in clear articulation and has that happened on Healthcare.gov?

Mr. PROVIDAKES. In the best world, you would love to have clear articulated requirements upfront that you can design to, build to, test to, and that would be great, although it is rare, but that would be great.

Mr. OLSON. OK, involving requirements with Healthcare.gov, has that been a problem?

Mr. PROVIDAKES. I am not sure of the number of requirements. I would think there were quite a number of requirements for Healthcare.gov.

Mr. OLSON. Ms. Bauer?

Ms. BAUER. I would—just having looked at it briefly, I would agree with——

Mr. OLSON. I apologize for that, ma'am.

Ms. BAUER. I would agree with the description of ideals—the ideal situation, however, I wouldn't have insight into the current situation because that involves the development of Healthcare.gov——

Mr. OLSON. OK.

Ms. BAUER [continuing]. Which is not within the scope of our contract.

Mr. OLSON. Mr. Amsler?

Mr. AMSLER. I would—ideal is—I agree with ideal. Again, we weren't involved in those aspects, so I couldn't speak to it.

Mr. OLSON. How about the program that ideal is sequential requirements design, build and testing, integration, revision between phases, and what the current situation is parallel stacking of all phases. Do you agree, Mr. Providakes? I apologize, sir, for not——

Mr. PROVIDAKES. That is fine. If——

Mr. OLSON [continuing]. Pronouncing—would idealism work?

Mr. PROVIDAKES. It would create significant challenges to the program office to deliver that.

Mr. OLSON. Has there been parallel stacking?

Mr. PROVIDAKES. It would be a significant challenge to do that.
Mr. OLSON. Ms. Bauer?
Ms. BAUER. I would agree with that statement.
Mr. OLSON. Mr. Amsler?
Mr. AMSLER. Agree.
Mr. OLSON. OK, how about interim integrated operations and testing is ideal. I think we all agree with that. And what has happened is insufficient time and scope of end-to-end testing. Would you all agree with those statements, yes or no?
Mr. PROVIDAKES. I guess in the context you put it, you are saying is there a limited end-to-end testing, and given the fact that you have a hard date, I would surmise they had limited time to end-to-end testing. It doesn't mean you couldn't have done it, it just meant there is limited time to do it.
Mr. OLSON. Ms. Bauer?
Ms. BAUER. Yes, generally I would agree. I would have no insight though into what the increments were as regards to schedule, but, you know, you could create milestones and achieve ideally just about any goal if you create the milestones and achieve them on the way to the goal.
Mr. OLSON. Mr. Amsler?
Mr. AMSLER. End-to-end testing for me is pure security. That is the world we live in, and that is the world that we only live in. We can achieve a lot testing along the way, but I would certainly—I always shoot for ideal. Ideal would be end-to-end testing.
Mr. OLSON. And ideal a limited initial launch or a full launch? Not ideal. Last question. Yes or no, do you agree with those statements? Launching at full volume is not very good, limited initial launch what we should be seeking?
Mr. PROVIDAKES. Well, limited launch increases the risk, obviously, than a full. It is an increased risk.
Mr. OLSON. Yes. Ms. Bauer?
Ms. BAUER. I would actually suggest that perhaps a limited launch would have had a lower risk, and that a full launch may have a larger risk, whatever system you would be deploying.
Mr. OLSON. Mr. Amsler?
Mr. AMSLER. I agree with Ms. Bauer's statement.
Mr. OLSON. Well said, sir.
And one final question. Again, I am not trying to put you on the spot, but with all your knowledge about how this program rolled out, are you comfortable putting yourselves' and your families', putting your personal information into Healthcare.gov?
Mr. PROVIDAKES. I have.
Mr. OLSON. You are comfortable? Yes.
Mr. PROVIDAKES. That is a personal choice that you have to make based on, in my case, where knowing the limited amount of personal information I put up there and other information, I feel comfortable personally, but that might not apply to everyone.
Mr. OLSON. Ms. Bauer, yes or no, ma'am, comfortable?
Ms. BAUER. Yes.
Mr. OLSON. Mr. Amsler?
Mr. AMSLER. I am actually very happy with my current health care.
Mr. OLSON. Oh boy, you are trying to open a hornet's nest there.

Mr. MURPHY. Well, too bad you can't keep it.

Mr. OLSON. That is my time.

Mr. MURPHY. What it comes down to. Gentleman's time has expired.

Ms. DeGette, you have a clarifying question?

Ms. DEGETTE. Thank you, Mr. Chairman.

The questions that Mr. Olson was asking you folks were on this McKinsey document that we spent so much time with the last witness talking about, tab 1 of the notebook. Have you seen that report before, Mr. Providakes?

Mr. PROVIDAKES. I am familiar with this report.

Ms. DEGETTE. OK. Ms. Bauer, have you seen it?

Ms. BAUER. No, I have not.

Ms. DEGETTE. And, Mr. Amsler, have you seen it?

Mr. AMSLER. I have not.

Ms. DEGETTE. OK. So, Mr. Providakes, the 2 of you—Ms. Bauer and Mr. Amsler, any answers you were giving were really just based on speculation, since you haven't seen it and weren't involved with it, is that right?

Ms. BAUER. Yes.

Ms. DEGETTE. Mr. Amsler?

Mr. AMSLER. That is correct.

Ms. DEGETTE. OK, Mr. Providakes, so Mr. Olson was asking you about some of these recommendations. This is from last spring. It was a snapshot in time. On page 4 of that report, at the bottom where he was talking about evolving requirements, multiple definitions of success, et cetera.

Mr. PROVIDAKES. Um-hum.

Ms. DEGETTE. The part he forgot to mention, which was the part also I noticed they forgot to mention when the previous witness was up, is the part that is in the box in bold type at the bottom of all of those current situation bullets, which says, CMS has been working to mitigate challenges resulting from program characteristics. Do you see that?

Mr. PROVIDAKES. I do see it.

Ms. DEGETTE. What does that mean to you?

Mr. PROVIDAKES. Well, it means to me that they recognize the risks and the challenges of the program, and they were looking at options or mitigation approaches that would minimize the risks.

Ms. DEGETTE. So CMS hired McKinsey to do an evaluation of the program and come up with some concerns that they could then work to mitigate. Is that right?

Mr. PROVIDAKES. Only what I—yes.

Ms. DEGETTE. And that is the same reason they hired your company to do security assessments, is to find places where there might be problems, and to make recommendations that they could then work to mitigate. Is that right?

Mr. PROVIDAKES. That is correct. Identify risks, mitigate risks.

Ms. DEGETTE. And in your view, at least the recommendations your company made, did they, in fact, work to mitigate those risks?

Mr. PROVIDAKES. In the context of the SCA, yes.

Ms. DEGETTE. Thank you very much, Mr. Chairman. I have no further questions.

Mr. MURPHY. OK, had you seen this document before today, Mr. Providakes?

Mr. PROVIDAKES. I am familiar of the document. It has been a while.

Mr. MURPHY. But—so you are familiar. So when they say they have been working to mitigate challenges, you are personally aware that some of these mitigations were taking place, or you are just saying so today?

Mr. PROVIDAKES. No, I had no idea of what mitigation—whether they took the recommendations of this or not——

Mr. MURPHY. I was curious because you were drawing a conclusion, but I didn't know if you had—so that is based upon——

Mr. PROVIDAKES. Based upon——

Mr. MURPHY [continuing]. Just a guess today, OK.

Mr. PROVIDAKES. Exactly, yes.

Mr. MURPHY. Quick thing. Mr. Amsler, while developing the security measures for the cloud environment, have you encountered any challenges at all?

Mr. AMSLER. Certainly lots of challenges along the way. Congressman, did you mean more implementing them or certain things?

Mr. MURPHY. Some things that are different from what you are used to here, or anything standing out to you that is a concern with regard to the cloud environment or the security there?

Mr. AMSLER. Well, the cloud in and of itself brings a unique set of challenges that any—us in the industry are all trying to deal with. It——

Mr. MURPHY. That is a system that you can't necessarily correct right now with a cloud environment. On its own, it is a secure concern.

Mr. AMSLER. Agreed. It is our biggest—one of our biggest challenges that we are facing as an industry today, that being the cyber security industry.

Mr. MURPHY. Who is in charge of that cloud environment?

Mr. AMSLER. Verizon Terremark is, and I assume you mean actually owns it——

Mr. MURPHY. Yes.

Mr. AMSLER [continuing]. And controls it.

Mr. MURPHY. And how difficult is it to develop these security measures while the system is being built?

Mr. AMSLER. That would not be ideal.

Mr. MURPHY. Do you have all the tools and capabilities now to successfully and fully monitor this system?

Mr. AMSLER. I am a unique animal in that I live, eat and breathe cyber security, and as a company, we do——

Mr. MURPHY. I understand.

Mr. AMSLER [continuing]. So we always strive for better. I am always striving to make it the best that I can.

Mr. MURPHY. Do you have all the tools now you need to fully monitor the system?

Mr. AMSLER. We have a set of controls that exceed any standard set of controls——

Mr. MURPHY. I understand you are trying to do a great job. I appreciate that. I am just trying to get a sense of have you been lim-

ited in any way in your ability to do all the things you would like to do with your excellent team in place?

Mr. AMSLER. There are some things that we have asked for that are not in place as of yet.

Mr. MURPHY. Tell me, such as what?

Mr. AMSLER. These were—they are very technical in nature. Again, we have a standard set of controls——

Mr. MURPHY. Sure.

Mr. AMSLER [continuing]. Or we are shooting for more.

Ms. DEGETTE. Mr. Chairman, we might want to have him give us that information——

Mr. MURPHY. Yes, could you let us know that?

Ms. DEGETTE [continuing]. And provide it.

Mr. AMSLER. I would be happy to.

Mr. MURPHY. Or is that something you would like to do in private instead of public? Would that be better?

Mr. AMSLER. I would be happy to get with my team and get with the——

Mr. MURPHY. I appreciate that. Ms. Bauer, do you have all the tools necessary to fully——

Ms. BAUER. Well, our answers are essentially the same because we are an integrated team.

Mr. MURPHY. I see.

Ms. BAUER. I would agree with Dave.

Mr. MURPHY. All right. And, Mr. Providakes, do you have all the tools necessary to fully do your work here?

Mr. PROVIDAKES. Well, we are in a slightly different role, but, yes.

Mr. MURPHY. I see. So let me ask this then, with regard to how things are. Have there been any attempts under what you have monitored, Ms. Bauer and Mr. Amsler, any attempts to hack into the system that you can tell?

Mr. AMSLER. Congressman, the simple answer is yes. The longer answer is I don't have an environment where it is not being attacked today, though.

Mr. MURPHY. I understand. So with regard to this, then, is the system now—are you saying that it is fully secure from external hackers trying to get in?

Mr. AMSLER. You know, I am never—we live in a world of not if but more when.

Mr. MURPHY. Um-hum.

Mr. AMSLER. That is the nature of the world we live in today. So I can never give you a guarantee that someone is not going to get in. It is probably going to happen at some point, but we have designed it to limit the damage and identify it as quick as possible.

Mr. MURPHY. So we can't at this point sign off and say the system is fully secure. It is an ongoing process, you are saying?

Mr. AMSLER. It is an always ongoing process. Today I feel comfortable with the capabilities we have put in place, but I am always striving for more.

Mr. MURPHY. I understand. And, Ms. Bauer, would you agree with that assessment?

Ms. BAUER. I would. Dave is answering it from a very——

Mr. MURPHY. You have to talk into the microphone, I can't hear you.

Ms. BAUER [continuing]. Very technical perspective, but I would say that from our perspective with regard to the tools and appliances we have in place, right now today, the system is secure. As Dave says, security is always evolving, it is always dynamic and ongoing, and we are always going to want to do better and keep on top of the latest technology, the latest appliances, so it will always be maturing. But as regards the scope of our contract and the appliances and tools and processes we have in place, we are confident——

Mr. MURPHY. I mean, I appreciate your standards of excellence, and I appreciate you understand this is an evolving process, but given the concerns for security, what I am hearing from you is nobody can really give 100 percent guarantee that this Web site is secure with regard to the data that it has in it, the personally identifiable information as people put those things in there. No one can guarantee that some hacker isn't going to try and get into it, and that they will continue to try and probe until they get through. Is that what you are saying?

Mr. AMSLER. But I also would say the same thing about Facebook or any banking Web site as well.

Mr. MURPHY. Sure.

Mr. AMSLER. It is just unfortunately the world we live in today.

Mr. MURPHY. I appreciate that. Same with you, Ms. Bauer?

Ms. BAUER. Yes, and I think that the critical factor is the rigor with which we have procedures in place to identify any risks, any vulnerabilities, and then work to mitigate them. And we have very robust procedures in place for that.

Mr. MURPHY. Very good. Well, I appreciate the comments from the panel today, and I ask unanimous consent that the written opening statements of other members be introduced into the record, and without objection, those documents will be in the record.

[The information follows:]

Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

Hearing on "Security of Healthcare.gov"

November 19, 2013

***

Statement for the Record
Hon. G.K. Butterfield

We can all agree that security of confidential personal information is critical to our constituents who are anxious to enroll in the Affordable Care Act.

The Hub and Federally-facilitated Marketplace eligibility and enrollment system have clearly complied with a robust regulatory framework of rules, regulations, standards, and laws. It is clear that because the ACA no longer allows insurance discrimination based on preexisting medical conditions, enrollees no longer need to divulge personal medical information as they used to when applying for insurance.

There is still much work to do to improve Healthcare.gov and get people enrolled by 2014. But the website complications are connected to user volume and not security concerns. It is encouraging that so many want to access the website and enroll in the ACA. We must focus our efforts on giving the 137,000 uninsured in my district the tools to access affordable care and spread the word to help get them enrolled. While security is paramount to my constituents, this hearing distracts from the true mission of getting more people quality care.

Mr. MURPHY. I also ask unanimous consent that the contents of the document binder be introduced into the record, and I authorize staff to make appropriate redactions. And without objection, the documents will be entered into the record with any redactions that staff determines are appropriate.

[The information appears at the conclusion of the hearing.]

Mr. MURPHY. So in conclusion, I would like to thank all the witnesses and members that participated in today's hearing. I remind members they have 10 business days to submit questions for the record, and I ask that the witnesses all please agree to answer promptly to the questions, and we will work out some mechanism to answer some of them in confidential, in-camera discussions.

And with that, this hearing is concluded.

[Whereupon, at 1:30 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

THE COMMITTEE ON ENERGY AND COMMERCE

MEMORANDUM

November 17, 2013

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on "Security of HealthCare.gov"

On Tuesday, November 19, 2013, at 10:15 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled "Security of HealthCare.gov." This hearing will focus on the issues surrounding the implementation of the Patient Protection and Affordable Care Act's (PPACA) health insurance exchanges and the security of HealthCare.gov.

I. WITNESSES

The following witnesses will testify at the hearing:

Panel I:

Mr. Henry Chao
Deputy Chief Information Officer and Deputy Director of the Office of Information Services
Centers for Medicare and Medicaid Services (CMS)

Panel II:

Mr. David Amsler
President and Chief Information Officer
Foreground Security, Inc.

Ms. Maggie Bauer
Senior Vice President, Health Services
Creative Computing Solutions, Inc. (CCSi)

Mr. Jason Providakes
Senior Vice President and General Manager
Center for Connected Government
MITRE Corporation (MITRE)

The Committee invited Verizon Terremark Federal (Verizon Terremark) to testify at the hearing. Verizon Terremark informed the Committee on November 16, 2013, that it declined the Committee's invitation to testify.

II. BACKGROUND

Over the last year, the Committee has asked Administration witnesses about the status of HealthCare.gov and whether the administration was ready for the launch of open enrollment on October 1, 2013. For example, in her testimony to the Committee on August 1, 2013, CMS Administrator Marilyn Tavenner assured the Committee that "CMS has been conducting systems tests since October 2012 and will complete end-to-end testing before open enrollment begins."

After the failed October 1 launch, the Committee opened an investigation into the implementation of the PPACA and the failed launch of the HealthCare.gov website. On October 10, 2013, the Committee sent letters requesting documents and certain information from the U.S. Department of Health and Human Services (HHS), CGI Federal, and Quality Software Services, Inc. (QSSI). After the Committee received documents indicating that the failure to conduct end-to-end testing prior to the October 1 launch presented certain security risks, the Committee sent letters on October 31, 2013, to HHS, MITRE, Verizon Terremark, CCSi, and Foreground requesting certain documents and information relating to the security of the Federally Facilitated Marketplace (FFM).

In response to these letters, the Committee has received initial document productions and Committee staff briefings from CMS officials and contractors. The Committee's investigation of the failed launch of HealthCare.gov is ongoing. Part II(A) of this memorandum provides background on the security-related aspects of Federal information technology systems development. Part II(B) provides a summary based on the documents and briefings provided to date to the Committee of how FFM applications and HealthCare.gov were tested for security and CMS' management of this process.

A. Overview of the Development of the Federally Facilitated Marketplace

PPACA implementation has involved multiple government agencies and contractors. Agencies such as the CMS, Internal Revenue Service, Social Security Administration, U.S. Department of Homeland Security, and the Office of Personnel Management are involved in the implementation of the PPACA exchanges. In addition, the HHS has entered into contracts with organizations to assist with the creation and operation of such exchanges, including the FFM. These contractors also are tasked with developing the applications that integrate the various components of the FFM.

Several contractors and various government officials play a role in the security of HealthCare.gov. The FFM is comprised of government agencies, user applications, data centers and State marketplaces. Each piece of the FFM infrastructure requires that security be imbedded

into the framework.[1] Ideally, functionality of the system complements the security, and the security is tested and improves as the system matures.[2]

Federally owned and operated IT systems must comply with several security standards. The Federal Information Security Management Act of 2002 (FISMA) outlines the basic requirements or framework for managing information security. Additionally, Federal IT systems must meet certain baseline security requirements. Agencies develop these baseline security requirements by establishing appropriate security controls and assurance requirements. Agencies have flexibility in applying the baseline security controls depending on the type of IT systems they manage.[3] Agencies, therefore, must customize the security controls to optimize mission requirements within the IT environment.[4]

Once security baselines or security controls have been developed and tailored to the needs of the IT system, the application developers and IT network service providers can integrate the security baselines into the overall system. Once the individual applications are developed, they are subject to a stress test known as a Security Control Assessment (SCA). The purpose of the security assessments is to identify security deficiencies and validate whether the application properly embeds the security controls.[5] These assessments may result in the recommendation of additional controls. Once a deficiency is identified, a finding is made and a level of risk is assigned to the finding. Additionally, if deficiencies are identified, they are mitigated if possible or a schedule is established in which the deficiencies are remediated.

After the assessments are completed and the systems and applications are integrated into the IT network, additional security measures ensure that the IT systems protections remain robust. Several examples of these measures include continuous monitoring, configuration management, systems access controls, and detection capabilities.

During the course of the Committee's investigation of the implementation of the PPACA, the Committee has identified several contractors that work with CMS to develop and validate the security controls and monitor system traffics with various tools and procedures. The following is a description of the security-related work performed by the FFM contractors who will testify at the November 19 hearing:

- MITRE was awarded a contract by CMS in November 2012. Under this contract, MITRE developed a Federal Facilitated Research and Develop Center (FFRDC) within CMS. One of the roles of the FFRDC was to develop the security control baselines for the exchanges. After MITRE developed these security controls, CMS disseminated the security controls to the contractors creating the applications for the FFM, which included CGI and QSSI. The contractors that developed the applications for HealthCare.gov were responsible for

---

[1] See generally, NIST Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.
[2] See generally, NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2013.
[3] Special Publication 800-53, Rev. 4, Section 1.4 Organizational Responsibilities. p. 4.
[4] Special Publication 800-53, Rev. 4, Section 1.4 Organizational Responsibilities. p. 4-5.
[5] NIST Special Publication 800-30, Rev. 1, 2012, provides guidance on the risk assessment process.

incorporating the security controls into the design of the applications. Once the applications were close to completion, MITRE performed the SCAs. The timing and the scope of the SCAs were determined by CMS. These SCAs test the applications' integration of the security baselines. Over the course of 2013, MITRE conducted four SCAs of FFM applications. For the FFM, the Enterprise Information Security Group (EISG) within the Office of Information Services (OIS) at CMS worked with MITRE to develop the risk assessments and oversees that they are conducted correctly.

- Verizon Terremark provides CMS with managed infrastructure services for the Federal Data Services Hub (DSH). Verizon Terremark was awarded its contract with CMS in November 2012. That contract will expire in March 2014. In this capacity, Verizon Terremark provides a quasi-private cloud computing environment which consists of hosting IT hardware within a virtualized network infrastructure housed in a large data center. The operating systems for the network infrastructure have security embedded in the physical architecture of their system. The applications developed by other contractors are then hosted on this infrastructure at the data center. CMS informed Committee staff that Verizon Terremark also provides external intrusion detection and perimeter security for the DSH.

- CCSi and Foreground Security monitor the perimeter firewalls and network devices for the eCloud. In August 2012, CCSi was awarded a small business contract, and Foreground Security is their subcontractor under the contract. In addition, these companies are responsible for scanning the code of the various applications in order to identify any security vulnerabilities. CCSi and Foreground Security are required to report any incidents they identify directly to CMS for remediation. They are also responsible for configuring CMS-furnished equipment within the Verizon Terremark eCloud.

Within CMS, responsibility for security is divided between two offices. Security related issues with the software applications, or those applications that users interact with on the exchanges and in the FFM, are managed by the Consumer Information and Insurance Systems Group, Marketplace Security Group (MSG) at CMS. The MSG oversees the remediation of security configuration flaws and vulnerabilities in the network infrastructure and the business applications. This group is headed by Monique Outerbridge, who reports directly to Deputy Chief Information Officer (CIO) Henry Chao. The other office responsible for security, EISG, establishes the security baselines and oversees the performance of the SCAs. The EISG is headed by Theresa Fryer. CMS Chief Information Officer Tony Trenkle worked closely with the personnel in EISG to develop the security baselines and conduct the SCAs. Mr. Trenkle's last day with the agency was November 15, 2013.

B. The Committee's Investigation of the Security of HealthCare.gov

Contracts for the design and development of two of the primary applications of HealthCare.gov – CGI and QSSI – were awarded by CMS in the fall of 2011. Approximately one year later, CMS awarded contracts to MITRE, CSSi, Foreground, and Verizon Terremark to develop other components of the FFM, including those related to security.

Beginning in January 2013, MITRE conducted a SCA of the Enterprise Identity Management (EIDM) application developed by QSSI. This SCA was completed on February 13, 2013. According to the SCA report drafted by MITRE, several high risks were identified and all were mitigated. The SCA also stated that as the EIDM was due for a new release, which added "significant functionality" and required a new SCA to be performed, "MITRE strongly recommends that CMS perform a comprehensive SCA of all subsequent releases of [the] EIDM . . . ."[6] Documents produced to the Committee to date do not indicate whether MITRE's recommendation to perform SCAs on subsequent releases of the EIDM was followed.

In June 2013, pursuant to its contract, MITRE conducted an SCA of the Exchange Consumer Web Services (ECWS) developed by Aquilent. According to MITRE's report issued on August 23, 2013, "[d]uring and after the assessment, Aquilent technicians focused their efforts on remediating the findings, with an emphasis on closing High and Moderate risk-level findings."[7]

In August 2013, MITRE conducted a SCA of the DSH. A MITRE report issued on this SCA on October 4, 2013, stated that MITRE identified several high risk findings and recommended that "[w]hile all findings will need to be addressed, findings representing a high risk to CMS data should be addressed first and closed or mitigating controls implemented to reduce the risk exposure to CMS."[8] The DSH received its Authorization-to-Operate (ATO) from CMS on September 6, 2013.

The final SCA before the October 1 start of open enrollment began in August 2013 and was completed on September 19, 2013. During this SCA, MITRE examined the Health Insurance eXchange (HIX) developed by CGI Federal. MITRE informed Committee staff during a briefing that CMS had to modify the scope of this assessment by limiting the systems and applications to be tested, because several of them were not complete. In its final report on this SCA, issued October 11, 2013, MITRE concluded that it was "unable to adequately test the Confidentiality and Integrity of the HIX system in full."[9] MITRE explained that, for purposes of the SCA, it was supposed to examine the "potential security risks to CMS" regarding applications and modules "not tested previously." MITRE went on to note that "[c]omplete end to end testing of the HIX application never occurred." Additionally, MITRE indicated in its report that at the time of the August-September SCA of the CGI HIX, several applications were still "being developed" and "impacted end to end MITRE test cases."[10]

The findings of MITRE's SCAs of the DSH and CGI's HIX necessitated that CMS issue certain authorizations prior to the October 1, 2013, launch of HealthCare.gov. On September 3, 2013, CMS CIO Trenkle issued an Authorization Decision for the FFM Qualified Health Plans and Dental modules. In this decision, the CIO determined that, based on the findings in the earlier SCA, "the risk to CMS information and information systems resulting from the operation of the

---

[6] CMS Enterprise Identity Management Security Control Assessment (SCA) Report, April 5, 2013.
[7] CMS Exchange Consumer Web Service (ECWS) Security Control Assessment (SCA) Report, August 23, 2013.
[8] CMS Federal Data Services Hub (DSH) Security Control Assessment (SCA) Report, October 4, 2013.
[9] CMS Health Insurance eXchange (HIX) August-September 2013, Security Control Assessment (SCA) Report, October 11, 2013.
[10] CMS Health Insurance eXchange (HIX) August-September 2013, Security Control Assessment (SCA) Report, October 11, 2013.

FFM information system is acceptable."[11] The decision to accept the risks for the site to operate was predicated on a list of mitigation measures that were to be completed in the future. The ATO listed the specific security findings and the schedule for mitigating those risks: five were to be completed in 2014, and the sixth in 2015.

As discussed earlier, the SCA conducted by MITRE of the CGI HIX in August and September revealed that no end-to-end testing was conducted prior to the beginning of open enrollment. During a briefing with Committee staff, CMS CIO Trenkle stated that given the high profile of the FFM and the risks associated with launching on October 1, 2013, it was his recommendation that CMS Administrator Tavenner sign an ATO after he informed her of the risks to the FFM. CMS CIO Trenkle also signed a separate Decision Memorandum that stated the mitigation plan that was in place because of these risks "does not reduce the risk to the FFM system itself going into operation on October 1, 2013."[12] In a separate briefing with Committee staff, Deputy CIO Chao explained that while he edited this memorandum, he was not familiar with the specific risks discussed in the memorandum because he had not seen the results of the SCA outlining the inability to test the system from end-to-end in a single environment.

On the recommendation of CMS CIO Trenkle, on September 27, 2013, CMS Administrator Tavenner signed a memorandum acknowledging that the FISMA required that the FFM "successfully undergo a Security Control Assessment (SCA)" and that "[d]ue to system readiness issues, the SCA was only partly completed." According to this memorandum, "[f]rom a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for the FFM." By signing this memorandum, CMS Administrator Tavenner recommended that CMS issue an "Authority-to-Operate" for six months that would allow the FFM to go forward with a mitigation plan in place and to perform a "complete SCA."

III. ISSUES

The following issues will be examined at the hearing:

- CMS' management of the security of the FFM and the roles and responsibilities of the various contractors for the security of the FFM;
- How the failure to perform complete end-to-end testing prior to the October 1, 2013, launch of HealthCare.gov affects the security of the FFM;
- CMS' current assessment of the security of HealthCare.gov and whether vulnerabilities have been identified.

IV. STAFF CONTACTS

[11] Authorization Decision for the Federal Facilitated Marketplaces (FFM) System, from Director of OIS, September 3, 2013.
[12] "Federal Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page," signed: T. Fryer, T. Trenkle, M. Snyder, dated: September, 27, 2013.

If you have any questions regarding this hearing, please contact Karen Christian, Carl Anderson, or Sean Hayes of the Committee staff at (202) 225-2927.

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
DOCUMENT BINDER INDEX

November 19, 2013

"Security of HealthCare.gov"

Exhibit Number	Document
1	Centers for Medicare & Medicaid Services-Red Team Discussion Document
2	Centers for Medicare & Medicaid Services, September 27, 2013 Memorandum; Federally Facilitated Marketplace-DECISION
3	Centers for Medicare & Medicaid Services, September 3, 2013 Memorandum; Authorization Decision for the Federal Facilitated Marketplaces (FFM) System
4	Centers for Medicare & Medicaid Services-Office of Information Services; Health Insurance eXchange (HIX) August-September 2013 Security Control Assessment (SCA) Report; Final Report, October 11, 2013
5	Email Exchange between CMS and MITRE, Subject: Onsite at CGI; July 27, 2013
6	Email From: Henry Chao To and CC: other CMS officials, Subject: House Oversight and Government Reform Committee-Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus, July 20, 2013
7	Email From: Henry Chao To: Monique Outerbridge, CC: other CMS officials, Subject: CGI Monthly Meeting Next Week, July 16, 2013

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Red Team

Discussion document

Red Team overview, objectives, and approach

The Red Team is:

- An independent team charged with "pressure testing" existing trajectory of the federal marketplaces
- Not a backwards looking effort or audit

Objectives	Approach
1 Develop a picture of the planned consumer experience over the first year	 Identify consumer paths; review and modify vignettes
2 Identify risks and threats to that picture	 Define stages of the journey and risks to each stage
3 Identify current and possible additional risk mitigation options	 Identify mitigation steps taken and other options to consider

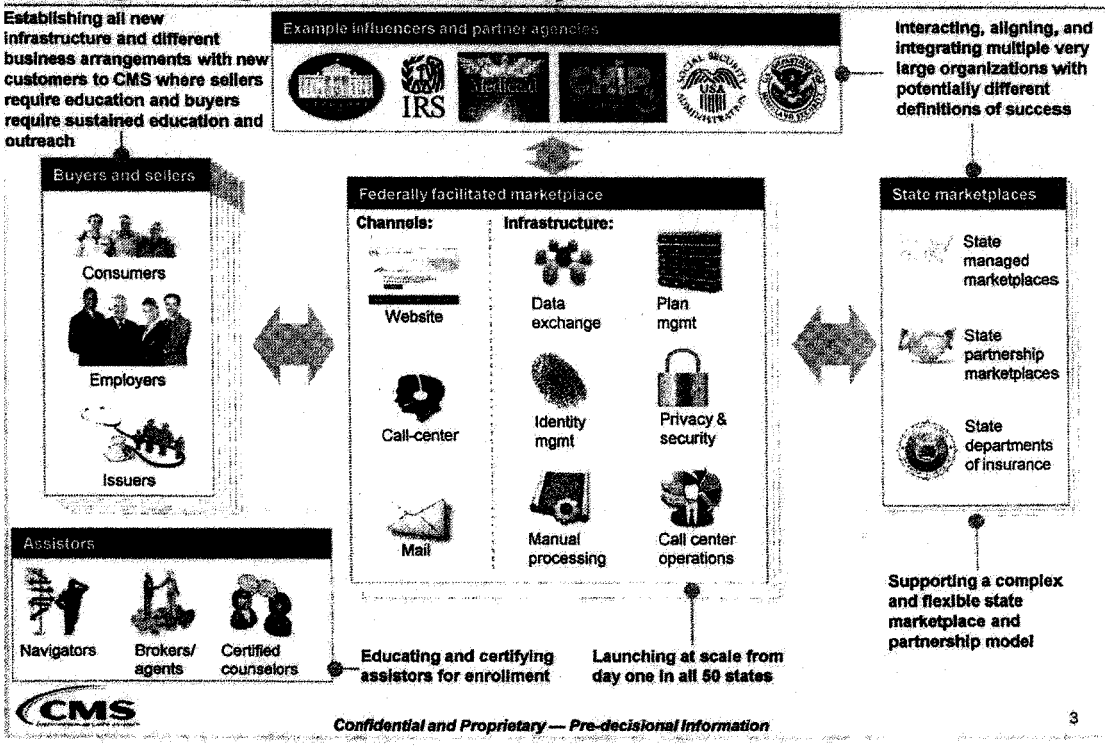
The working group determined that extending the go-live date should not be part of the analysis and therefore worked with a boundary condition of Oct 1 as the launch date

Overview of the Red Team sources of insight

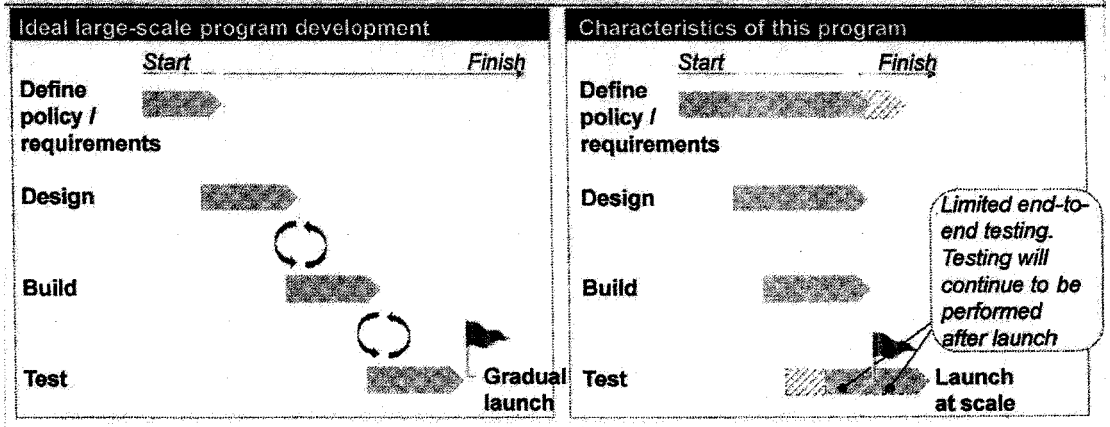
- **Reviewed 200+ documents and artifacts**, including operational designs and reports, implementation plans, workload forecasts, contract-related documents, and management reports and schedules
- **Interviewed ~40 people** across 6 CMS/HHS Offices, Centers, and FFRDC and Federal partner agencies
- **Participated in select meetings and working sessions**, including weekly operations meetings and OIS working sessions

Per the scope of the review, the Red Team did not include outside interviews (e.g., issuers, states) nor access to operating work products (e.g., SOPs, computer code, or programs)

Implementing the health insurance marketplaces is a unique challenge in magnitude and complexity



Programs of this type ideally have a sequential planning, design, and implementation process with significant testing and revision



Description of ideal situation:

- Clear articulation of requirements & success metrics
- Minimized dependency on third parties
- Sequential requirements, design, build, and testing
- Iteration and revision between phases
- End-to-end integrated operations and IT testing
- Limited initial launch

Current situation:

- Evolving requirements
- Multiple definitions of success
- Significant dependency on external parties/ contractors
- Parallel "stacking" of all phases
- Insufficient time and scope of end-to-end testing
- Launch at full volume

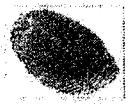
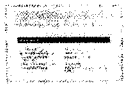
CMS has been working to mitigate challenges resulting from program characteristics

EC/0005

Example: Fully automated

Hypothetical consumer profile: Mike

- Mike is married with a two year old son, lives in Maine, and wants to enroll his family in insurance
- He works at an engineering company with 30 employees that does not offer employer sponsored coverage and his household income is $49,000 (~250% of FPL)
- Mike has worked for the same company for 3 years and his household income has not changed significantly in that period

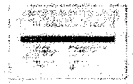
	Consumer experience	Approximate time required		Consumer experience	Approximate time required
	Mike contacts an insurance agent to enroll in coverage; the agent begins an application online on Mike's behalf	30 mins		**The broker helps Mike select a plan and enroll**; Mike makes an initial payment to issuer	30 minutes
	Mike satisfies ID verification, residency status check, and income verification	5 mins		**Total elapsed time for Mike to enroll**	**<1 day**
	The application web site indicates Mike's subsidy amount	Real time		Mike receives a letter from the insurance company indicating his date of initial coverage	Goal: 1 – 2 weeks

Example: Manual (high complexity)

Hypothetical consumer profile: Charles

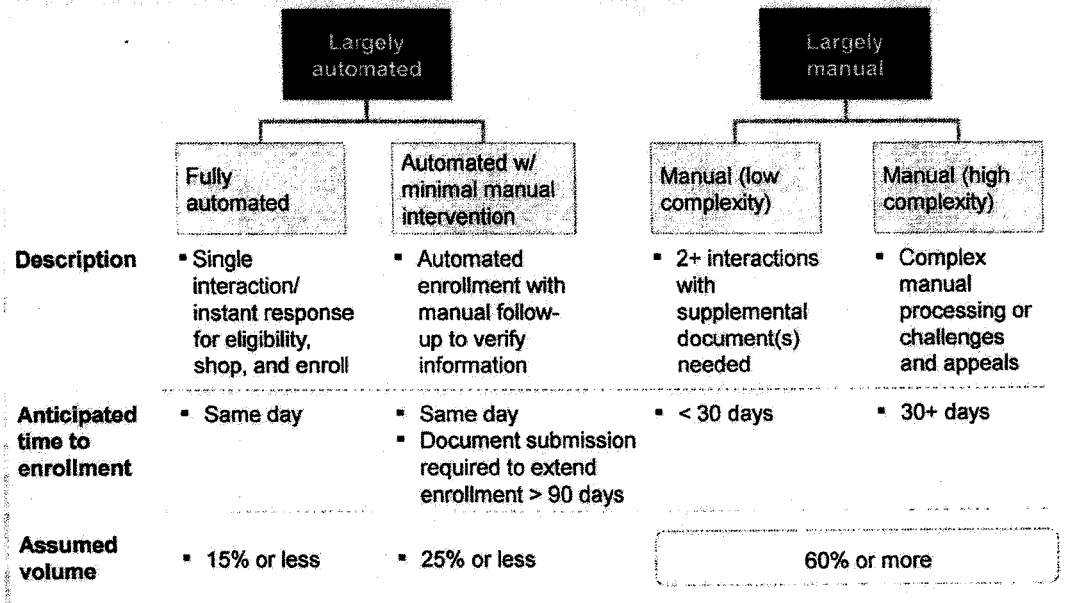
- Charles is single male making $15,500 (~135% of FPL) working part-time as a handyman
- He recently left the military and no longer has insurance coverage through TRICARE
- Charles lives in Texas and would like to apply for insurance through the marketplace
- He has very little income budgeted for health care and wants to be sure he receives the full amount of subsidy for which he qualifies

	Consumer experience	Approximate time required
	Charles completes a paper application	1 hour
	He receives a letter indicating he may qualify for Medicaid; his information is sent to the Texas Medicaid program	3-4 weeks
	Charles receives notification that upon state review, he does not meet state-specific Medicaid requirements, which he forwards to the FFM	3-4 weeks
	Due to a system lag, he receives notification that he is ineligible to buy on the FFM because he appears to have TRICARE[1] coverage	1 month

	Consumer experience	Approximate time required
	He calls the call center to challenge the notification and is asked to send documentation that he no longer has coverage	Real time
	The FFM confirms his eligibility and makes a final subsidy determination	3-4 weeks
	**Call center operator helps Charles enroll** in a plan and he makes initial payment	Real time
	Total elapsed time for Charles to enroll	**13 – 16 weeks**
	Charles receives a letter from the insurance company indicating his date of initial coverage	Goal: 1 – 2 weeks

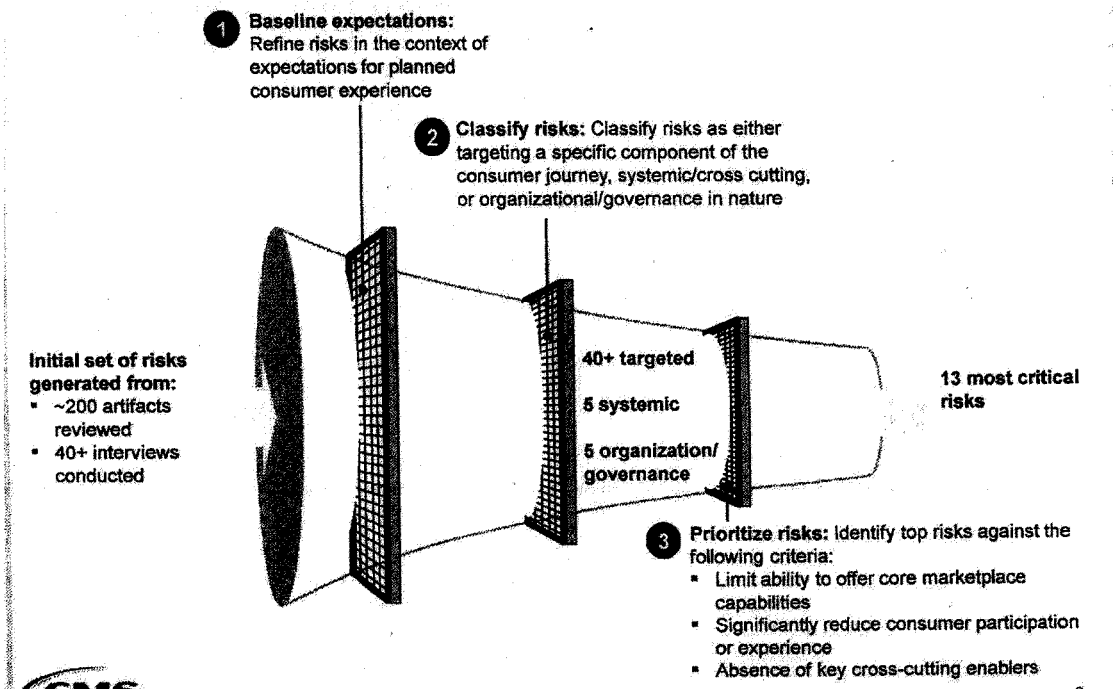
1 TRICARE real-time checks may not be available on Day 1

Complexities of the marketplace and its implementation drive four primary experiences for consumers enrolling on FFM ESTIMATES



Note: Volume assumptions based on CBO estimates with adjustment for FFM share, resulting in 5M enrollees in individual market and 1.2M enrollees in SHOP. Volume numbers do not include expected Medicaid enrollees or exemptions. See appendix for methodology.

Risk prioritization approach



CMS

EC/0009

Most critical risks to marketplace implementation efforts—
Core marketplace functionality / Experience and participation

	Risk	Root cause drivers
Core marketplace functionality	A Marketplaces unavailable with system failure	▪ Data Hub / FEPS are single points of failure ▪ Limited end-to-end testing prior to launch
	B Long manual processing times	▪ Potentially undersized contractor eligibility support team ▪ Potential protest of June 1st contract ▪ Higher than expected manual processing volumes
	C Failure to resolve post-launch issues rapidly	▪ Compressed testing window and volume uncertainty ▪ Inter- and intra-agency response teams not yet in place
	D No viable marketplace in large-volume SBM states	▪ Large-volume SBM states (i.e., NY, CA) too big to fail ▪ High risk of federal IT/Ops resource overload if pivot needed
	E Plans not approved and loaded in selected markets	▪ Lack of time/resources for State DOI's ▪ SBM pivots may miss 4/30 data load deadline ▪ Issuers may not design and offer plans
Experience/Participation	F Lack of inter-agency consensus on verification standards results in unexpected tax debt to consumer and unrecoverable excess federal subsidies in 2015	▪ No inter-agency consensus on verification standards ▪ Subsidies calculated with less accurate income ▪ Accepting business risks to meet deadlines
	G Inaccurate or incomplete financial management systems	▪ Financial management system release in December ▪ Limited testing time and resources prior to launch ▪ Due to focus on enrollment, limited focus on financial management
	H No call center enrollment channel or long waits	▪ Call center tools linked to enrollment IT systems ▪ Minimal integration/testing time prior to 10/1 launch ▪ Significant risk of higher call volumes

Most critical risks to marketplace implementation efforts— *Cross-cutting enablers*

Risk	Root cause drivers
I Fast, targeted, locked-down decisions are needed for implementation effort	▪ Matrix management and consensus decision making ▪ No clear roles, responsibilities and processes for making change ▪ No single empowered decision-making authority ▪ Lack of a "shared definition of success"
J Indecision about Version 1.0 requirements in select areas	▪ Less than 180 calendar days – design still presumed to be open ▪ Drives development churn and compressed timelines ▪ Materially higher risk of system instability
K Lack of end-to-end operational view of interdependencies	▪ Operational interdependencies among groups ▪ No end-to-end business process view across agencies or fully within agency ▪ Difficult to identify/address critical integration gaps
L No critical path transparency (inter- and intra-agency)	▪ Lack of transparency and alignment on critical issues ▪ Critical path drives coordination of end-to-end efforts ▪ Lack of visibility into critical milestones across agencies ▪ Staff still engaged in program design
M Budget uncertainty and timing prevents execution of plan	▪ Many functions are contractor dependent ▪ Core contracts not awarded due to budget ▪ Hampers ability to hire/resource critical path activities

Options that could be implemented to help mitigate key risks

	Mitigation type	Mitigation options
1	***Align on initial release and transition to solving for stability*** 	▪ Prioritize and lock down scope for "version 1.0" ▪ Conduct fully integrated end-to-end test of version 1.0 ▪ Continue to enhance plan to develop an "operations command center" and response team
2	***Take tactical actions in targeted areas*** 	▪ Determine readiness of SBM implementations ▪ Mitigate risks related to Call Center and Eligibility support contracts ▪ Define broker/agent and issuer direct enrollment model ▪ Manage demand through targeted outreach ▪ Accelerate decision-making on using IRS tax data for verification of income
3	***Streamline decision making process and manage critical path*** 	▪ Name a single implementation leader (COO/DCOO) and implement associated governance process to: – Manage critical path – Create transparency on critical issues ▪ Finalize budget and release funds

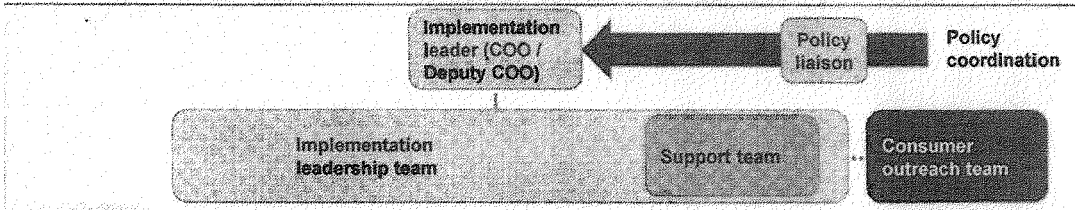
Implementing these mitigation options does not guarantee success

1 Top areas where requirements need to be defined and "locked down" by April 30

Decision	Description
ID proofing (IRS)[1]	▪ Requiring AGI as a shared secret will likely increase the amount of time needed to complete an application for enrollment but will provide IRS with more confidence in a user's identity when returning federal tax information
Household consent (IRS)[1]	▪ Current taxpayer privacy rules require identity verification for each tax return that is retrieved to construct the household income and family size
Marketplace operating models	▪ Determine how each marketplace operating model should function (i.e., SBM and different flavors of partnership models, e.g., Utah) with specific description of business rules for each marketplace variation
Issuer direct enrollment	▪ Define entire end-to-end business flow (registration, authentication, handoffs of information, types of data, SLAs) by which issuers will direct enroll consumers into plans and
Agent / broker enrollment	▪ Define process by which agents and brokers can enroll consumers ▪ Agent/broker training and certification (for safeguarding Federal Tax Information) need to be developed and implemented
Financial management	▪ All financials system management processes and calculations need to be defined including: APTC and CSR aggregations across exchanges, internal accounting systems, monthly receipt and reconciliation of enrollment reports, collection of marketplace fees, and payment of APTC and CSR

1 ID proofing and household consent need to be finalized by April 12

3 An implementation leadership team and a consumer outreach team could drive implementation progress



Responsibilities

Implementation leadership team

- **Expedite decisions** on critical path and Version 1.0
  - If consensus cannot be reached, the leader will decide or escalate
- **Regulate issues affecting IT and Ops build**
  - Reduce number of governance bodies to one
  - All decisions impacting build must flow through this team
- **Report directly** to the Administrator and Secretary
- **Brief White House** on implementation progress
- **Requests from policy staff** must flow through the policy liaison

Support team

- **Track project status** from all stakeholders
- **Create an integrated managerial view** across key milestones
- **Surface risks** to facilitate resolution
- Provide **analytic capability** to support rapid decision-making

Consumer outreach team

- **Coordinate** with the implementation leadership team
- **Drive consumer outreach**
- **Coordinate outreach efforts** across CMS, HHS, the White House and partner organizations

Membership

Implementation leadership team

- 1 representative each (CMS Administrator to select):
  - CCIIO
  - CMCS
  - CMCHO
  - OC (same as Call Center)
  - OIS
  - SSA
  - IRS

Support team

- 3-4 dedicated FTEs
- Additional support as needed

Consumer outreach team

- Sr. Advisor to the Administrator
- OC Director
- 1 representative each:
  - Call centers
  - Regional offices
  - CCIIO
- Others TBD

CMS needs specific support from HHS and the White House to successfully operationalize the marketplaces

Critical action	Deadline
1. Agree to lock down open requirements by 4/30[1] and shift all other new requirements or changes to existing requirements into version 2.0	▪ Mon, 4/8
2. Implement new governance process to support effective operational execution	▪ Fri, 4/12
3. Determine desired demand strategy	▪ Fri, 4/12
4. Align on shared metrics for success	▪ Fri, 4/12
5. Lock down all funding sources for year 1 operations	▪ Mon, 4/15
Distribute funds as early as possible to match contracting schedule	▪ Ongoing
6. Communicate pivot plan to SBM states	▪ Mon, 4/21

1 ID proofing and household consent need to be finalized with IRS by April 12

DATE:

TO: Marilyn Tavenner

FROM: James Kerr, Consortium Administrator for Medicare Health Plans Operations
Henry Chao, Deputy Chief Information Officer & Office of Information Services Deputy Director

SUBJECT: Federally Facilitated Marketplace–DECISION

ISSUE:

The Federal Information Security Management Act (FISMA) requires that the various Federally Facilitated Marketplace (FFM) systems - Enterprise and Eligibility (E&E), Financial Management (FM), and Plan Management (PM) successfully undergo a Security Control Assessment (SCA). Due to system readiness issues, the SCA was only partly completed. This constitutes a risk that must be accepted and mitigated to support the Marketplace Day 1 operations.

BACKGROUND:

CMS utilizes independent and specialized contractors to test the security readiness of its systems. Testing of the Marketplace has been on-going since inception as part of the CMS Expedited Life-Cycle process with the latest security testing occurring in September of 2013. As with all new systems which are pending launch, there are inherent security risks with not having all code tested in a single environment, finally, the system requires rapid development and release of hot-fixes and patches so it is not always available or stable during the duration of testing,

From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM. Although throughout the three rounds of SCA testing all of the security controls have been tested on different versions of the system, the security contractor has not been able to test all of the security controls in one complete version of the system.

The risk associated with issuing an ATO for the FFM will be reduced by instituting a two-part mitigation plan.

First, CMS will implement the following security processes for the first year of operation of FFM:

- Establish a dedicated security team under the Chief Information Officer (CIO) to monitor, track and ensure the mitigation plan activities are completed. The CIO and the Chief Information Security Officer (CISO) will report weekly on the progress to the Health Reform Operations Board;

Page 2 – The Administrator

- Monitor and perform weekly testing of all border devices, including internet facing web servers;
- Conduct daily/weekly scans using the CISO's continuous monitoring tools
- Conduct a full SCA test on FFM (E&E, FM and PM) in a stable environment where all security controls can be tested within 60/90 days of going live on October 1st.

Second, CMS will migrate the Marketplace systems to CMS' Virtual Data Center (VDC) environment in Q1-2014. This environment has been through a full security assessment and has an authority to operate.

RECOMMENDATION:

Issue an Authority-to-Operate (ATO) for six months and implement the mitigation plan. The six month period will allow the Marketplace to normalize its development activities while enabling the security team to closely monitor activities and perform a complete SCA.

DECISION:

Approved [redacted] Date SEP 27 2013

Disapproved_____ Date_____

Marilyn Tavenner

Attachment: Federally Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
[redacted]

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Federally Facilitated Marketplace Decision Memo
Risk Acknowledgment Signature Page

We acknowledge the level of risk the Agency is accepting in the Federally Facilitated Marketplace (FFM). The mitigation plan does not reduce the risk to the FFM system itself going into operation on October 1, 2013. However, the added protections do reduce the risk to the overall Marketplace operations and will ensure that the FFM system is completely tested within the next 6 months.

Reviewer [redacted] Date 9-27-2013
Teresa Fryer

Reviewer [redacted] Date 9-27-2013
Tony Trenkle

Reviewer [redacted] Date 9-27-2013
Michelle Snyder

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services

[redacted]

OFFICE OF INFORMATION SERVICES

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

MEMORANDUM

DATE: SEP 3 2013

TO: Director,
Consortium for Medicare Health Plans Operations (OA/CMHPO) and Acting Deputy Center Director for Operations, Center for Consumer Information and Insurance Oversight (CCIIO)

FROM: Chief Information Officer and
Director, Office of Information Services (OIS)

SUBJECT: Authorization Decision for the Federal Facilitated Marketplaces (FFM) System

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Federal Facilitated Marketplaces (FFM) System is a ***Moderate*** level system located at the Terremark Datacenter in Culpeper, Virginia. The system maintains records used to support all Health Insurance Exchange Programs established by the Centers for Medicare & Medicaid Services (CMS) under the health care reform provisions of the Affordable Care Act (Public Law 11-148). FFM will help qualified individuals and small business employers shop for, select, and pay for high-quality, affordable health coverage. Exchanges will have the capability to determine eligibility for coverage through the Exchange, for tax credits and cost-sharing reductions, and for Medicaid, Basic Health Plan (BHP) and Children's Health Insurance Program (CHIP) coverage. As part of the eligibility and enrollment process, financial, demographic, and (potentially) health information will flow through the Exchange.

On August 8, 2013, you certified the controls for the system and submitted along with your certification the other required documentation necessary to obtain an Authorization to Operate (ATO) for FFM.

I have determined through a thorough review of the authorization package that the risk to CMS information and information systems resulting from the operation of the FFM information system is acceptable predicated on the completion of the actions described in the attachment. Accordingly, **I am issuing an Authorization to Operate (ATO)** for the FFM information system to operate in its current environment and configuration until **August 31, 2014**. The current configuration includes only the Federal Facilitated Marketplaces Qualified Health Plans (QHP) and Dental modules. This system is not authorized to establish any new connections or interfaces with non-CMS FISMA or other non-CMS connections without prior approval during the period of this ATO. An impact analysis must be conducted for any system changes implemented after the issuance of this ATO. Any major modifications that affect the security posture of the system will require an appropriately scoped security controls assessment and issuance of a new ATO.

The security authorization of the information system will remain in effect until the indicated expiration date if the following conditions are maintained:

(i) Required periodic security status reports for the system are submitted to this office in accordance with current CMS policy;
(ii) New vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk that is deemed unacceptable; and
(iii) The system has not exceeded the maximum allowable time between security authorizations in accordance with Federal or CMS policy.

The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones (POA&M) tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates. This office will monitor all POA&M items submitted during the period of authorization.

If you have questions, please contact Teresa Fryer, Chief Information Security Officer (CISO), at [redacted] The DISPC team is also available to support staff level questions at [redacted]

[redacted]

Tony Trenkle

Attachment

cc:
Mark Oh, Director OIS/CIISG/DHIM
Darrin Lyles, ISSO, OIS/CIISG/DSMDS
Teresa Fryer, CISO, Director OIS/EISG
Michael Mellor, Dep. CISO, Dep. Director OIS/EISG
Desmond Young, OIS/EISG/DISPC
Jessica Hoffman, OIS/EISG/DISPC
James Mensah, OIS/EISG/DISPC

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services

[redacted]

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

CENTERS FOR MEDICARE & MEDICAID SERVICES

Office of Information Services

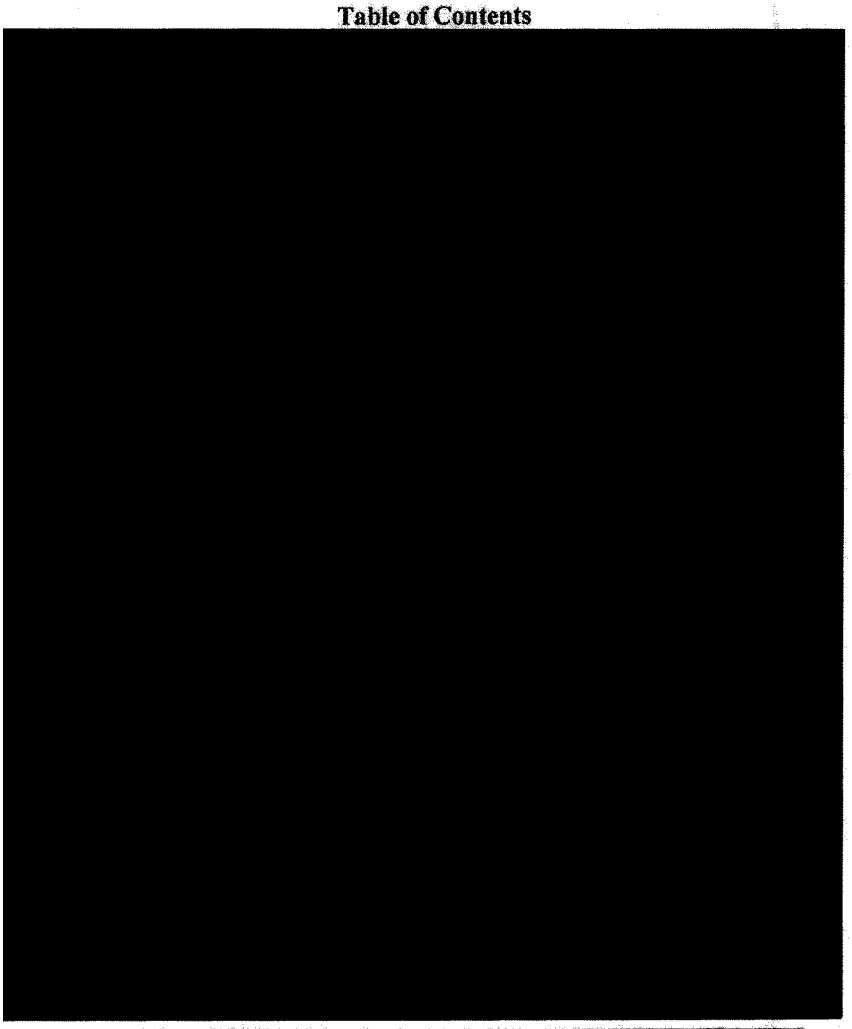
[redacted]

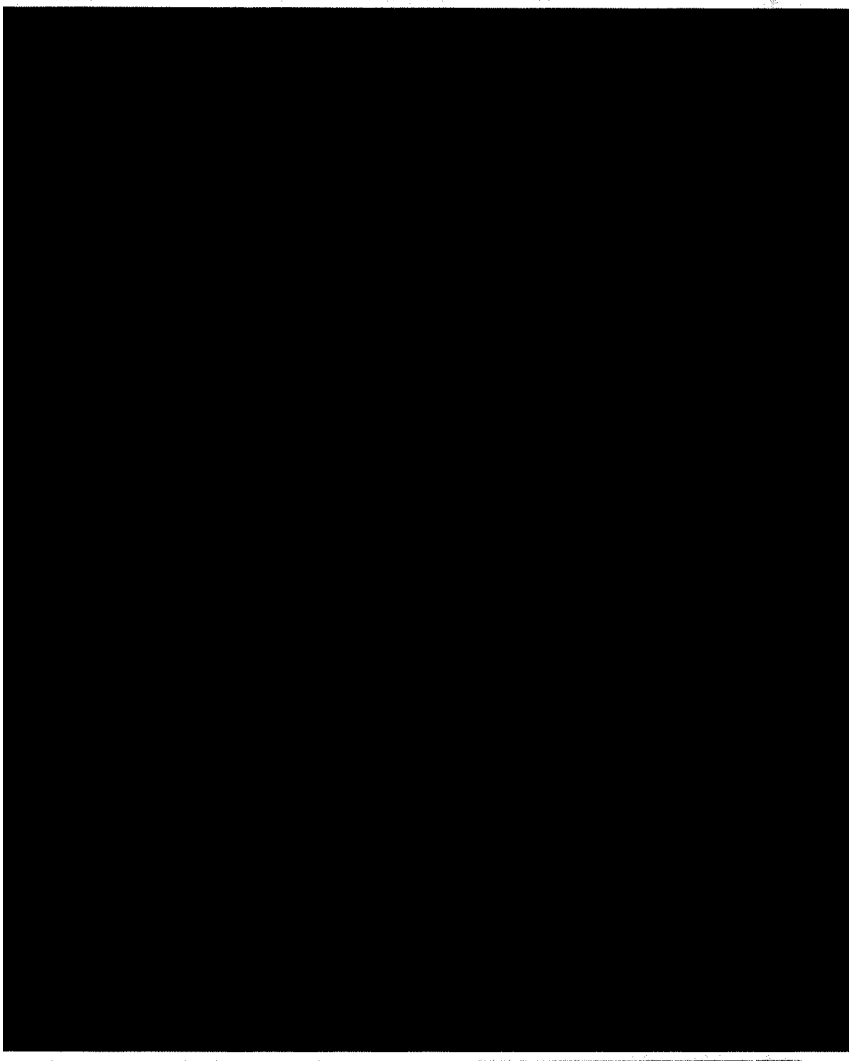
Health Insurance eXchange (HIX) August – September 2013 Security Control Assessment (SCA) Report

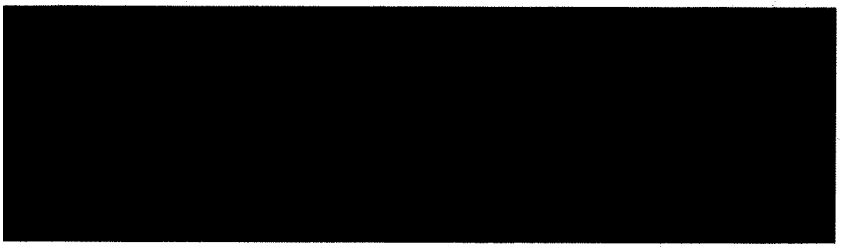
Final Report

October 11, 2013

Table of Contents



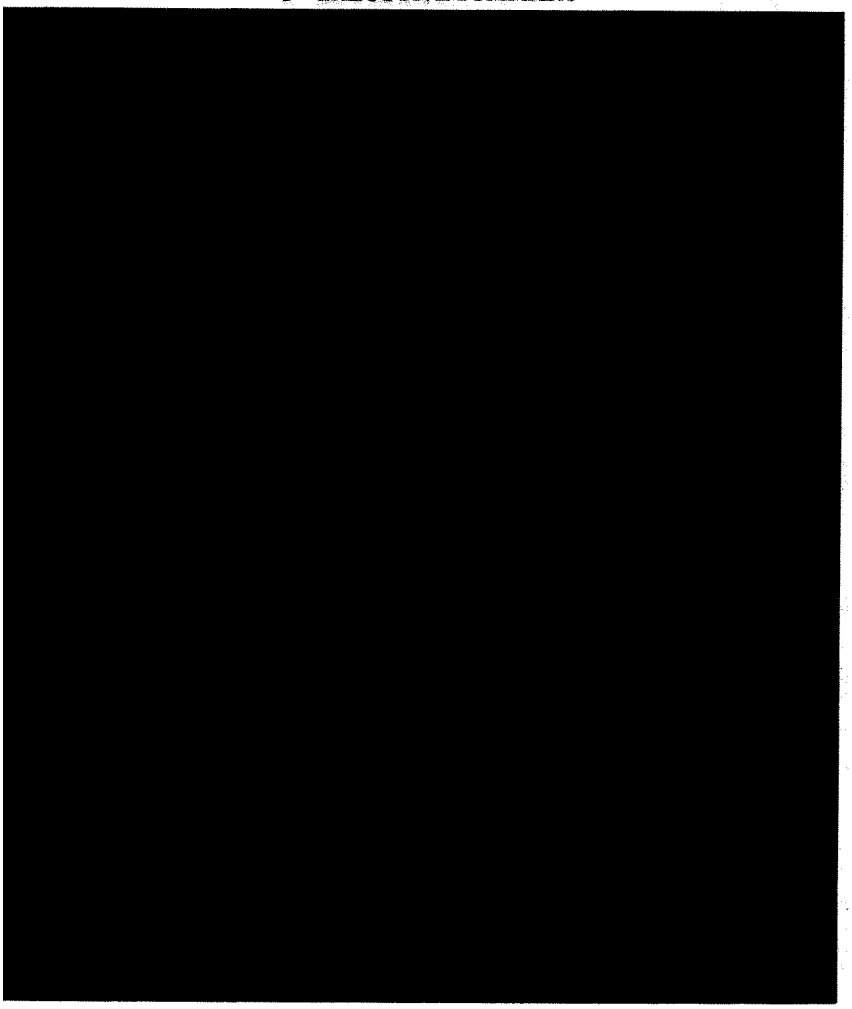


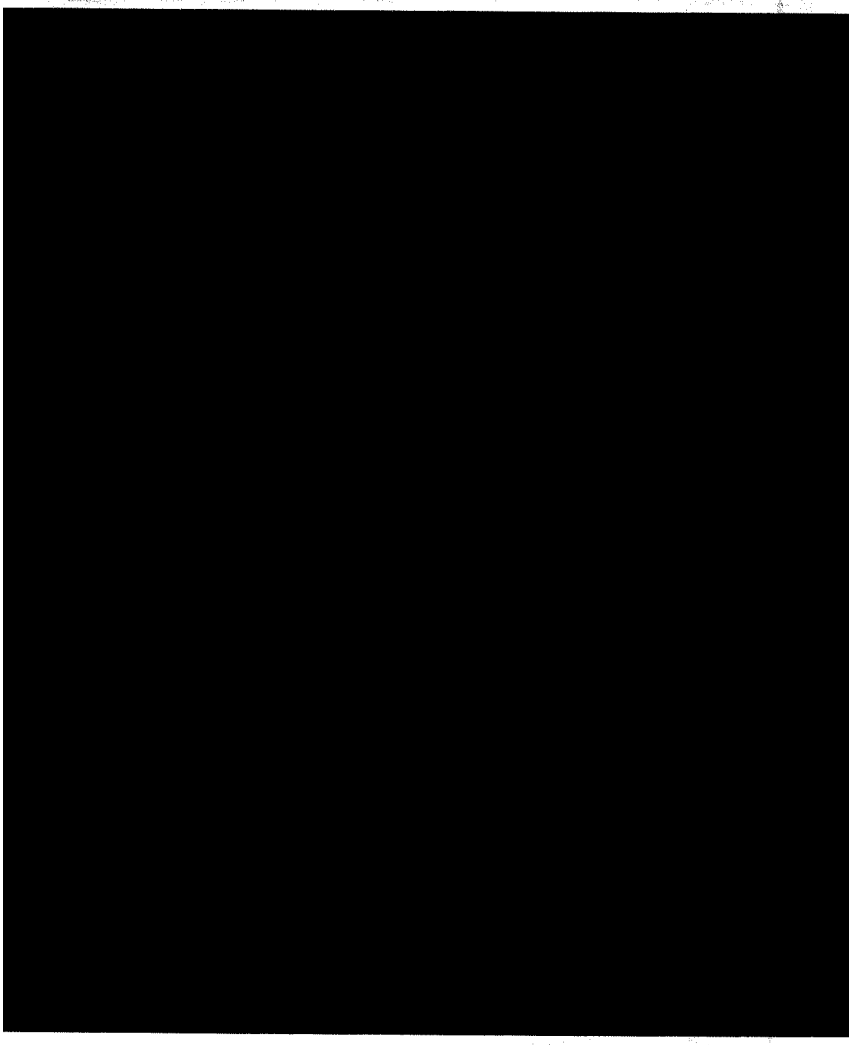


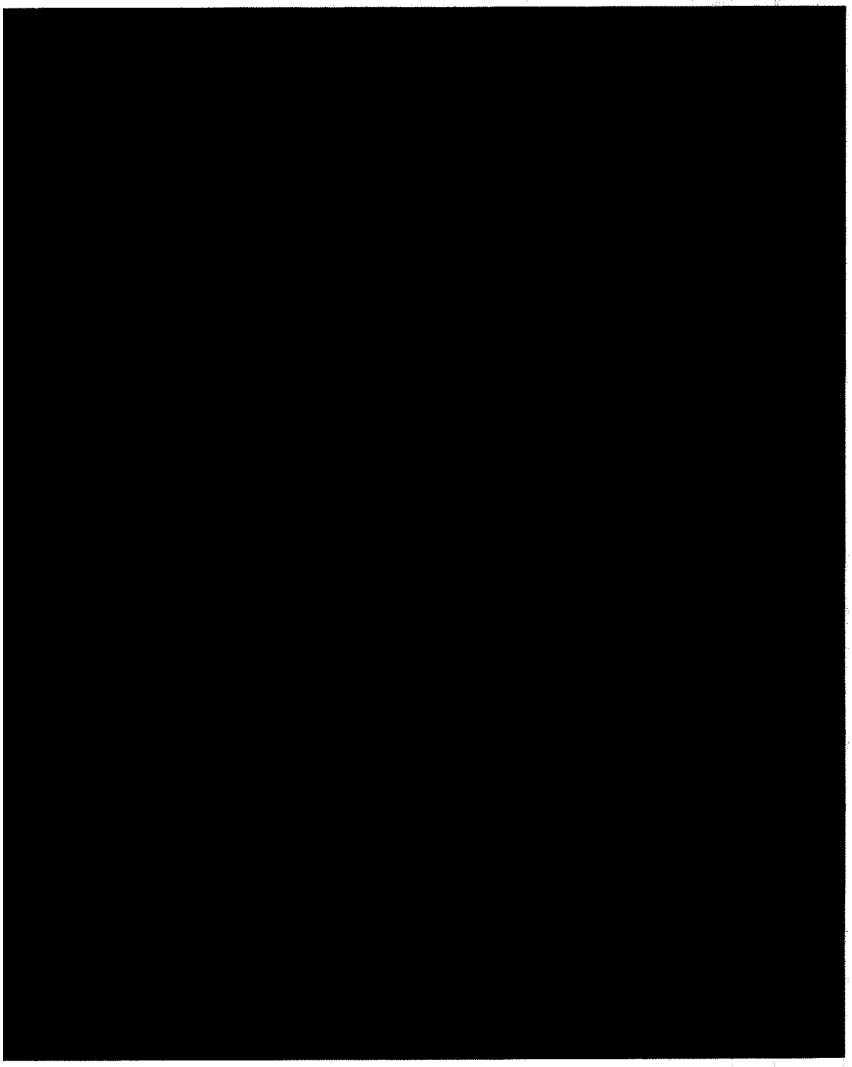
List of Tables

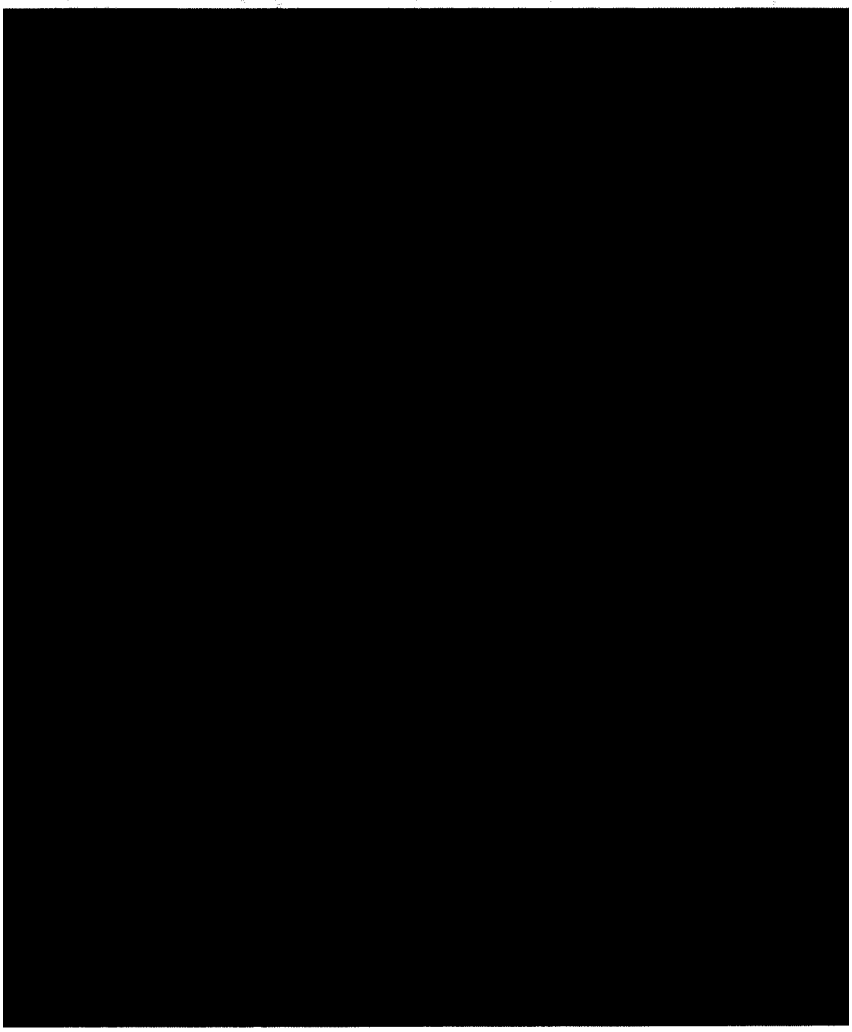
List of Figures

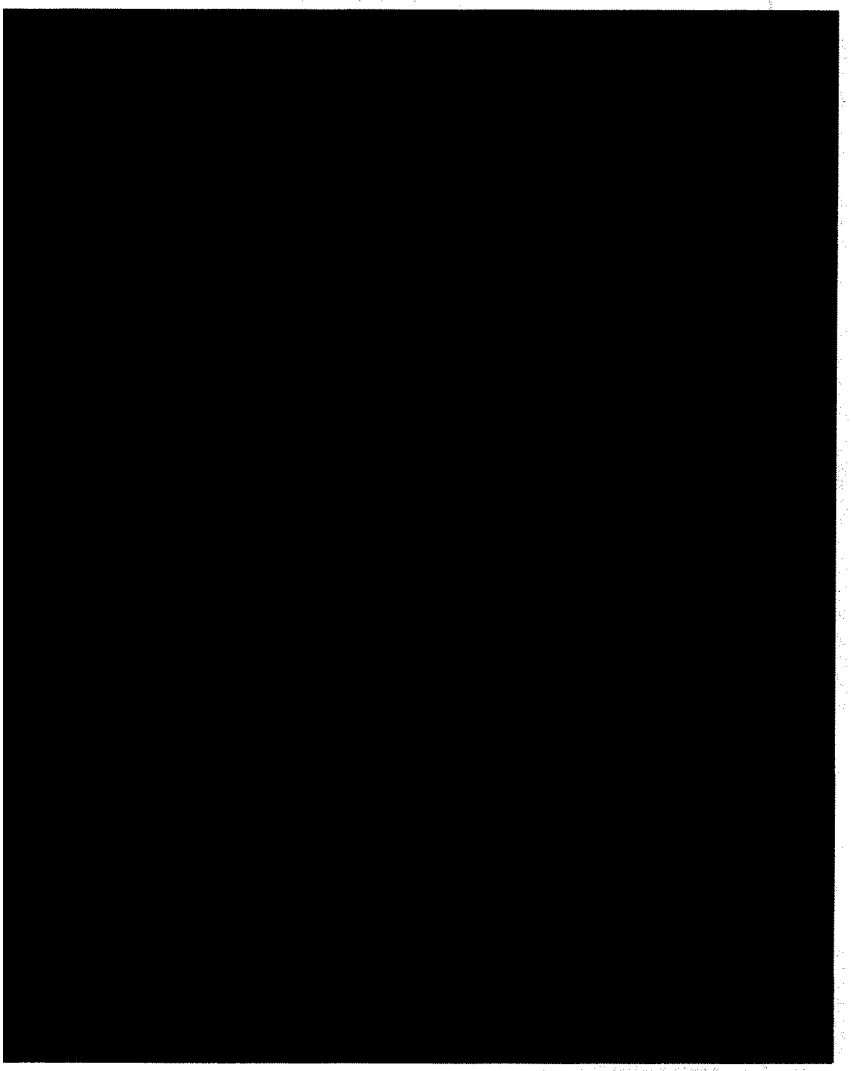
1 EXECUTIVE SUMMARY

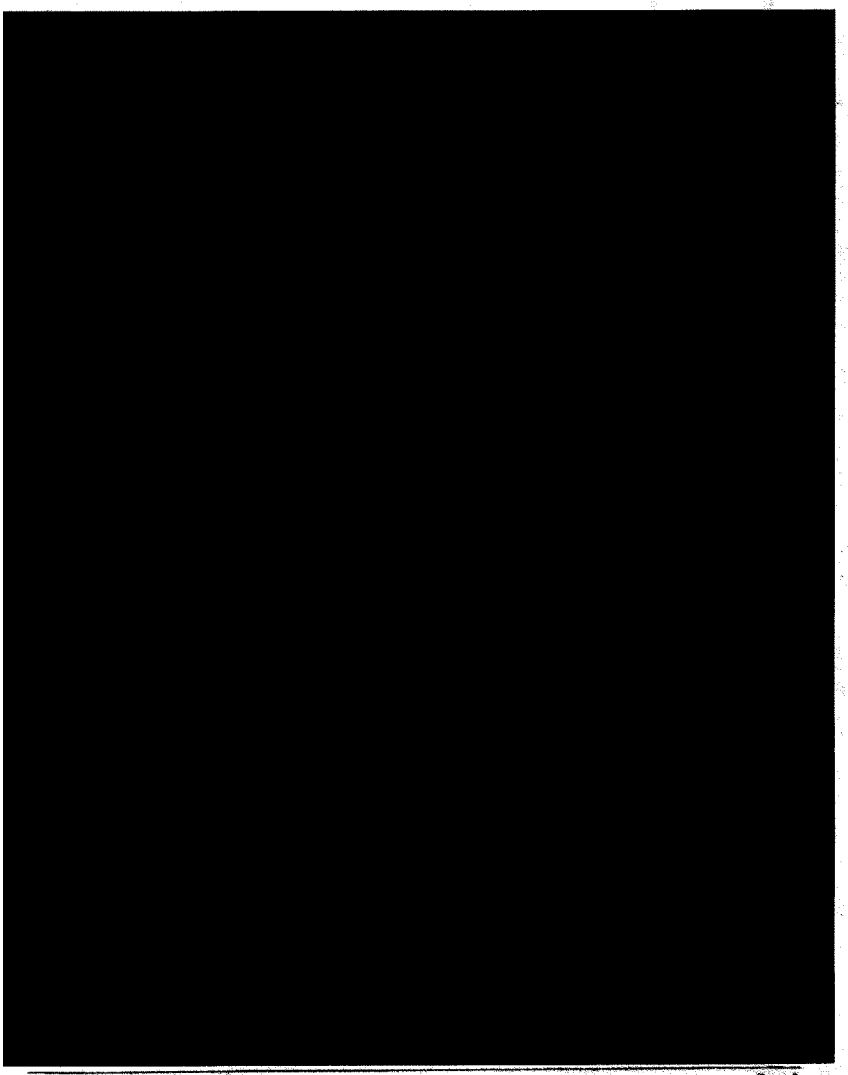


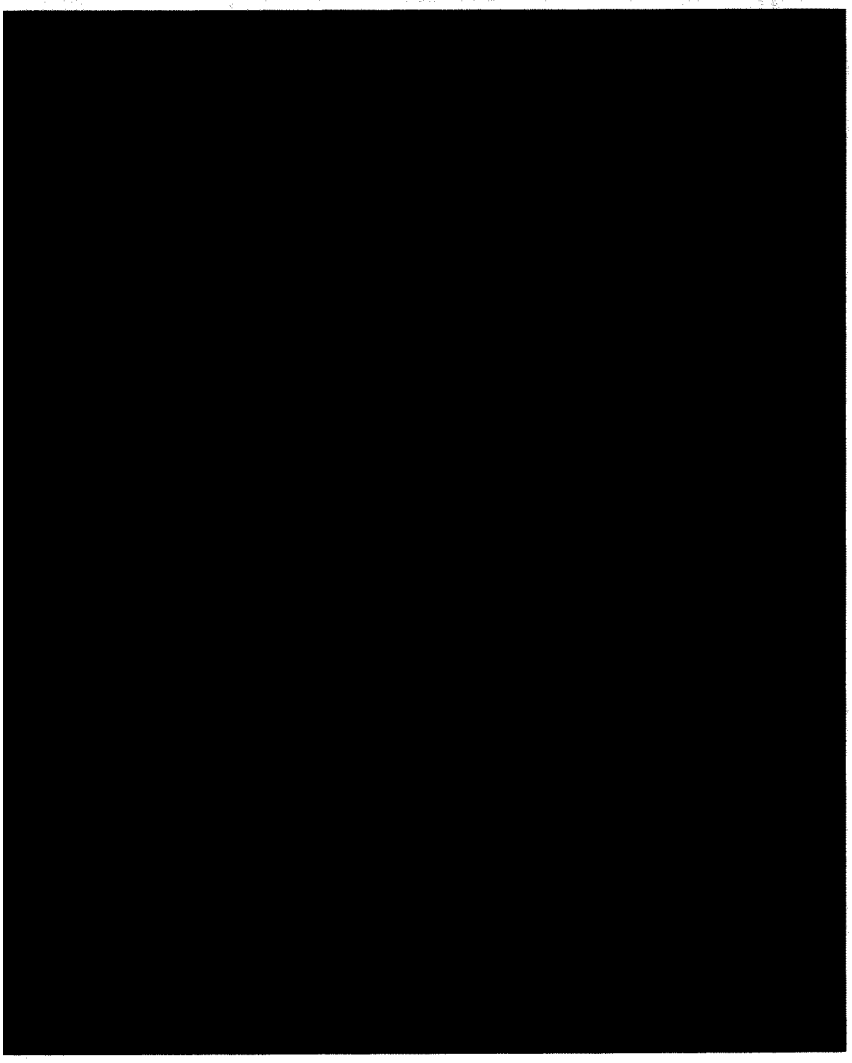


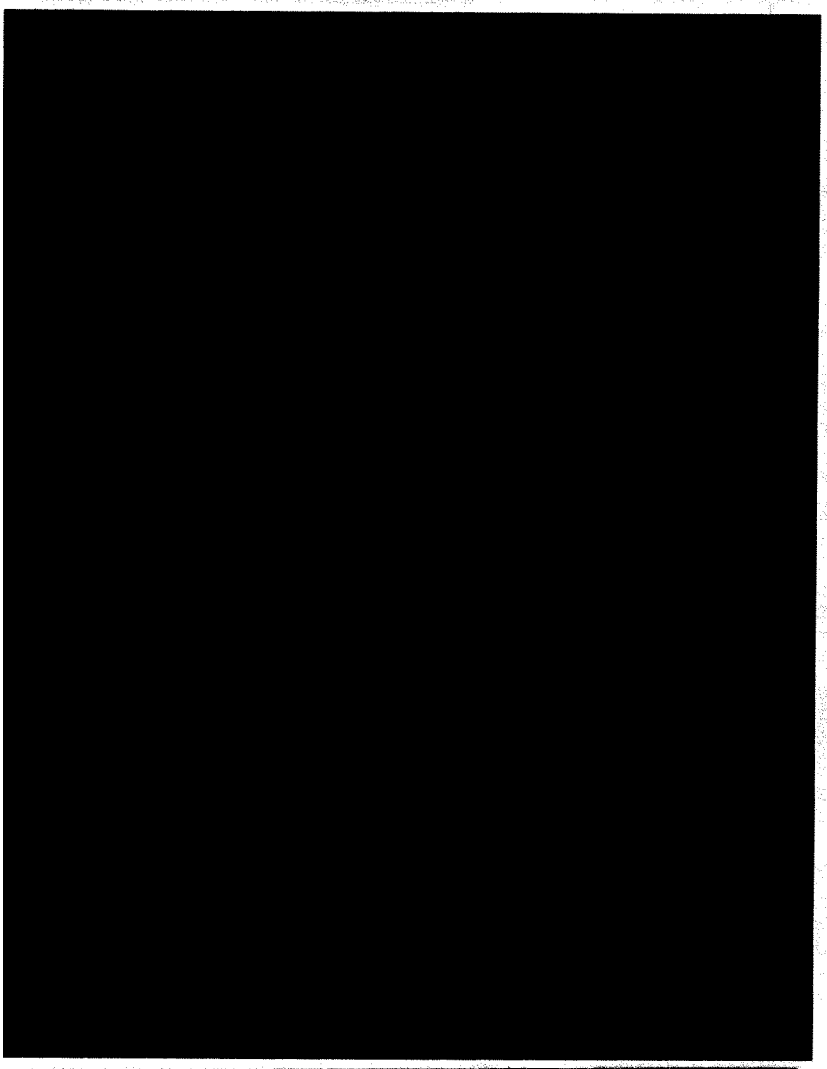


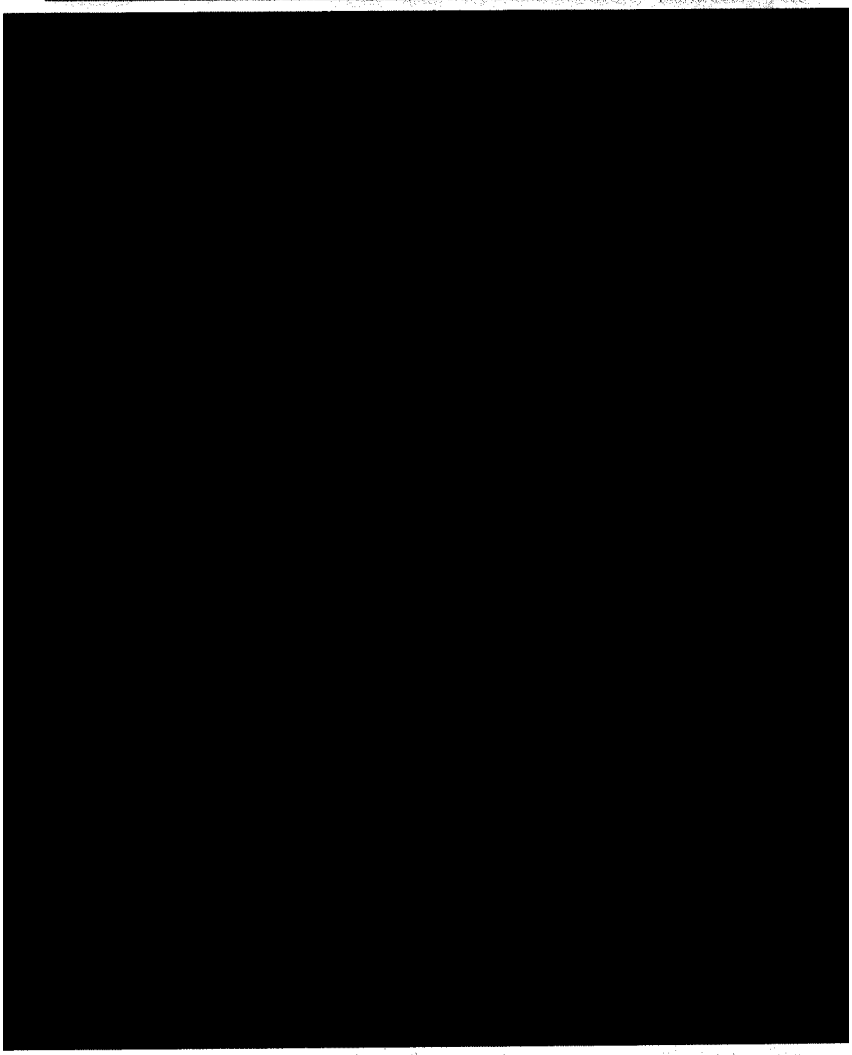


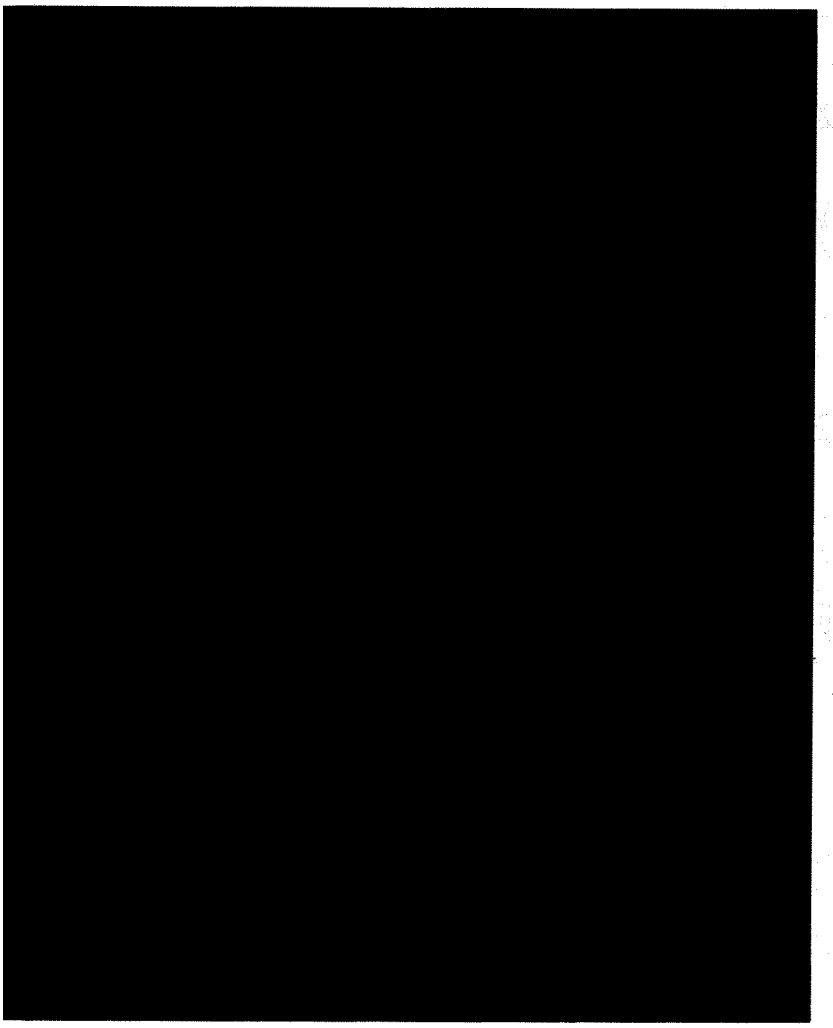


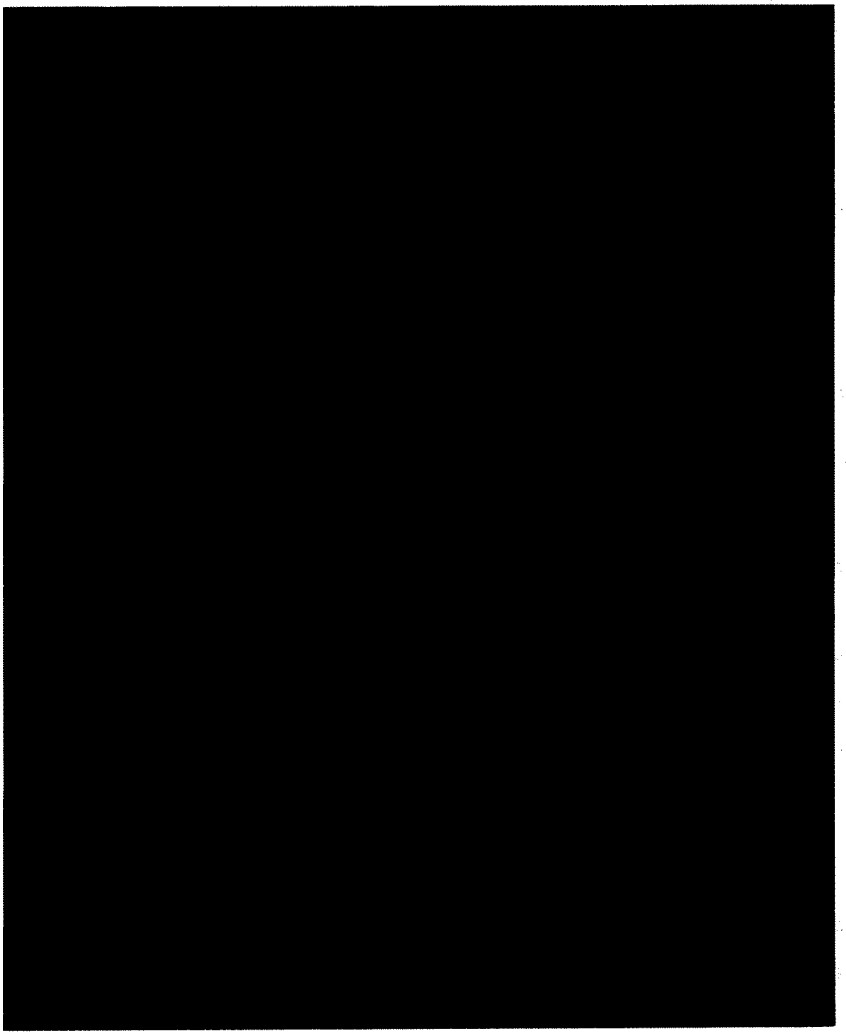


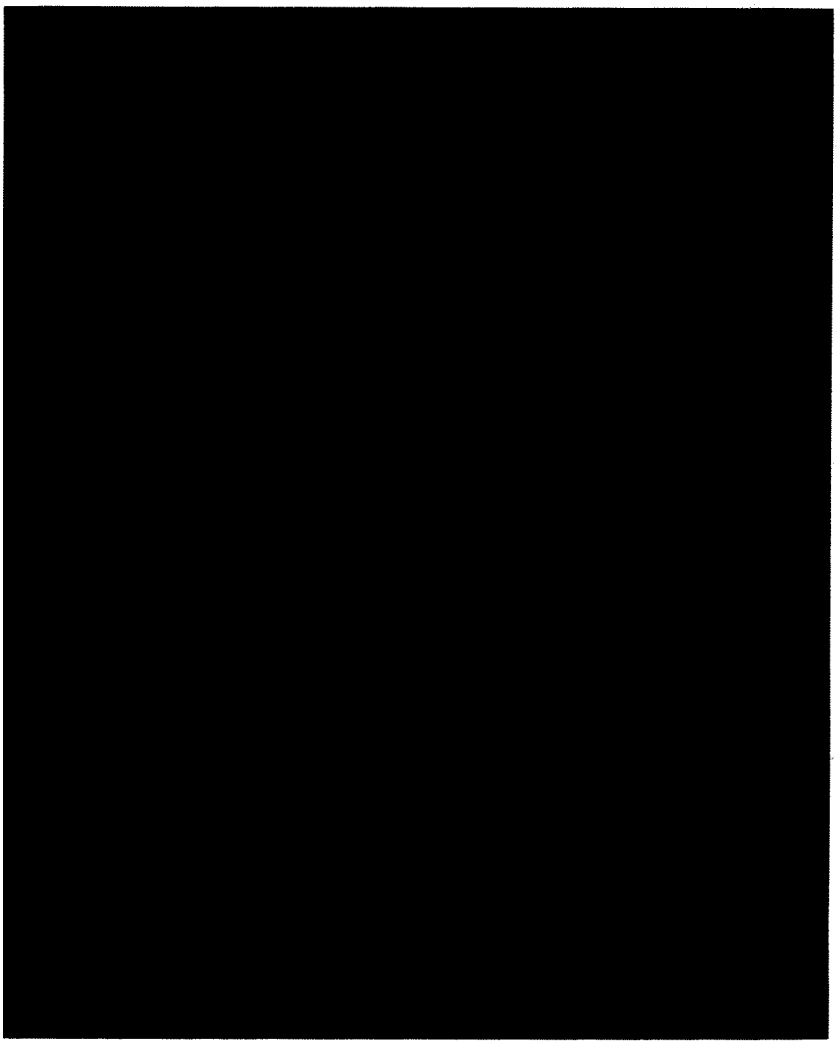


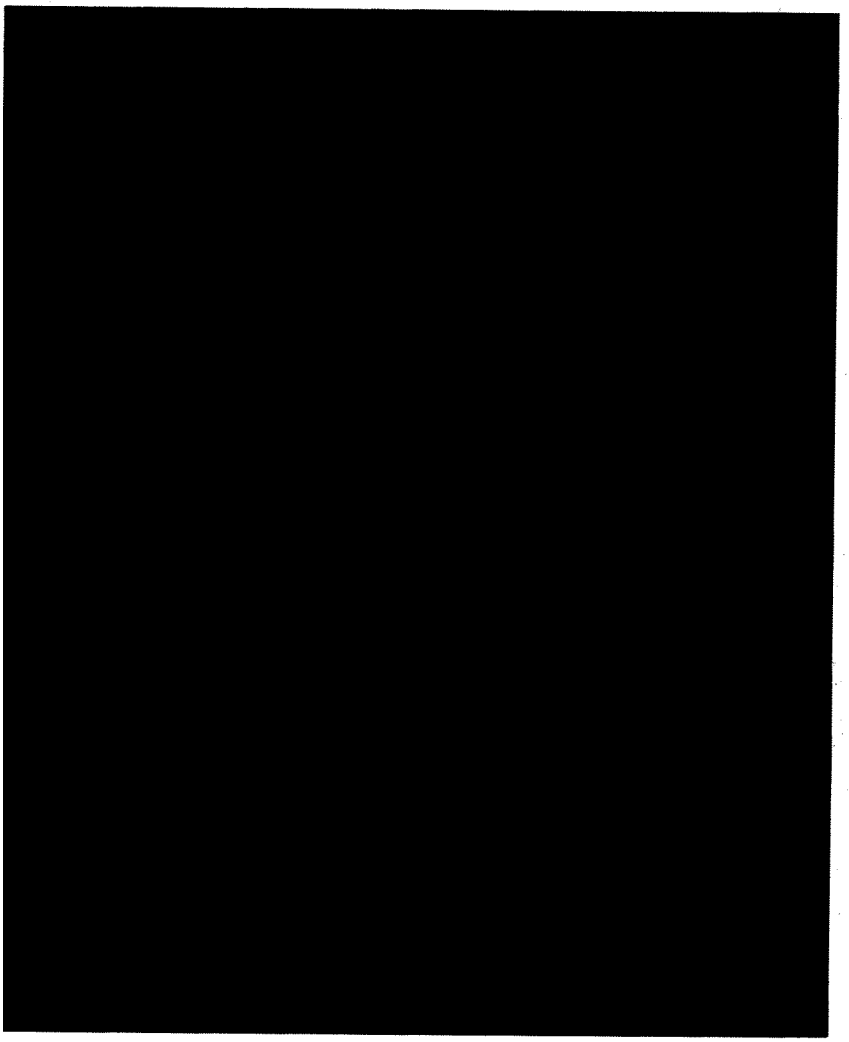


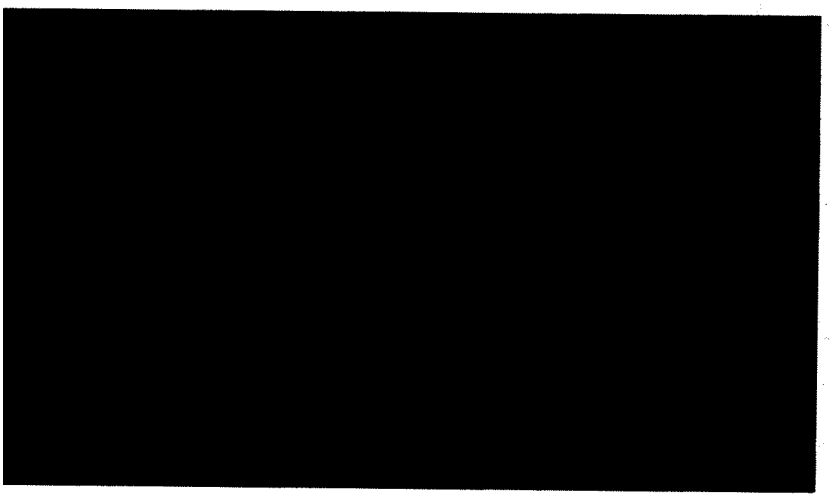




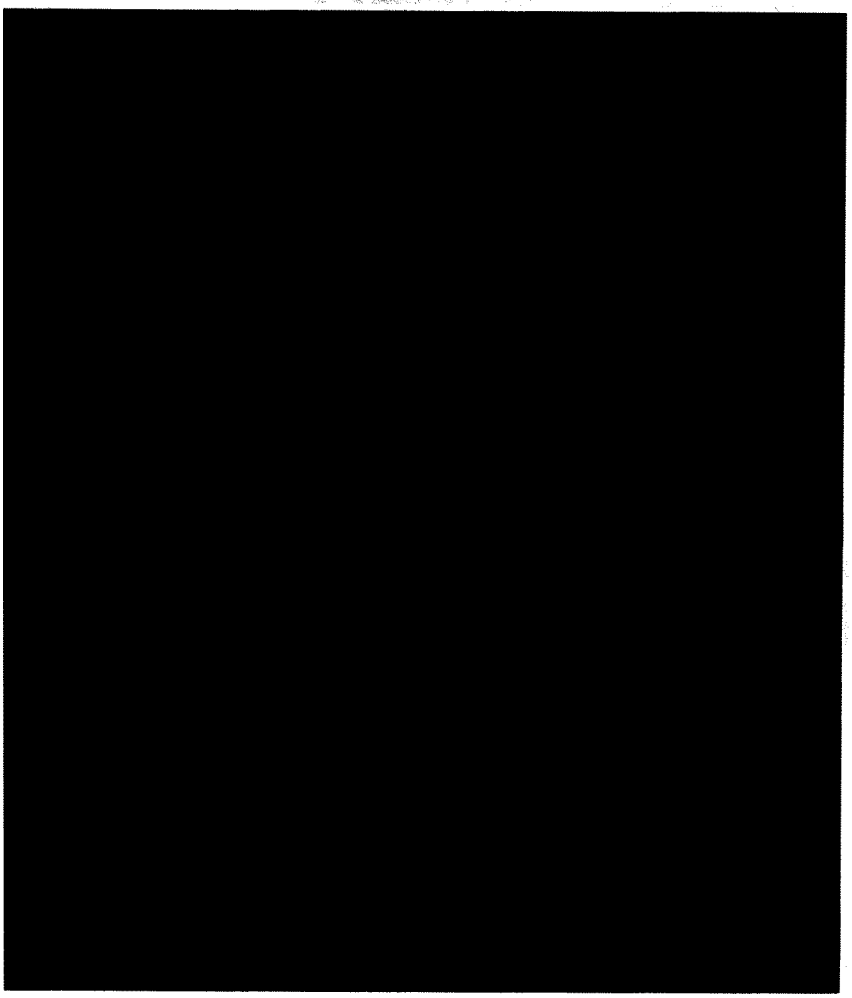


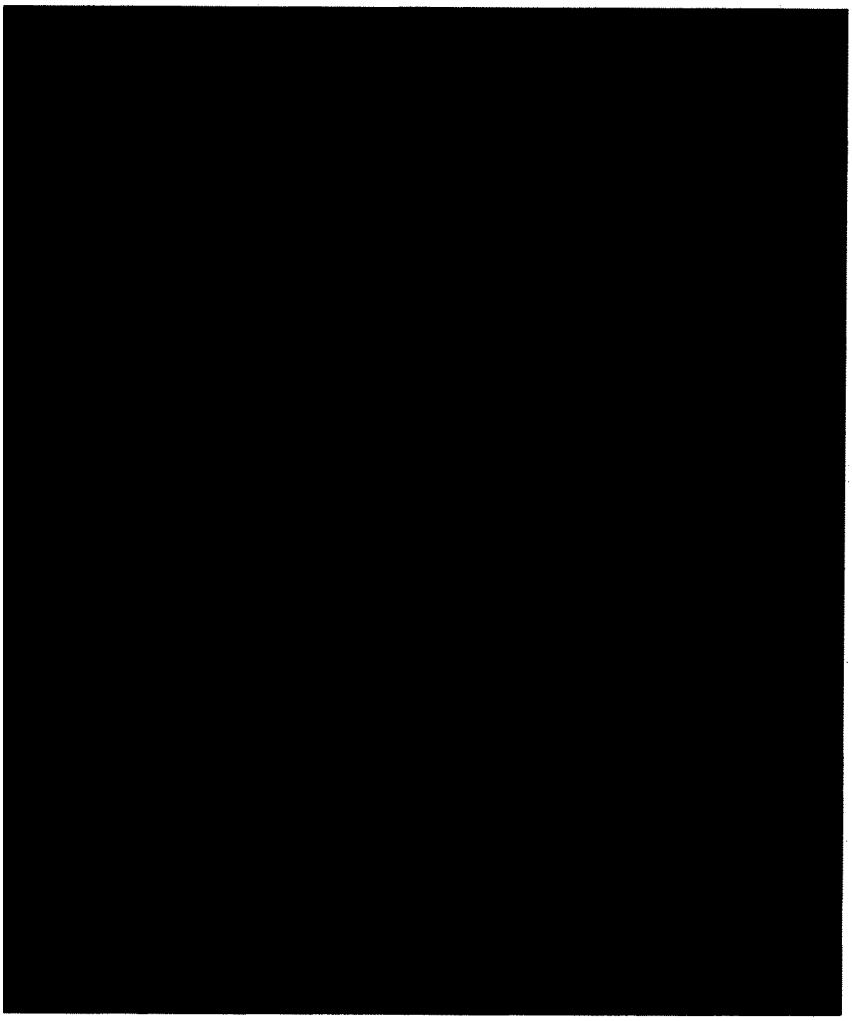


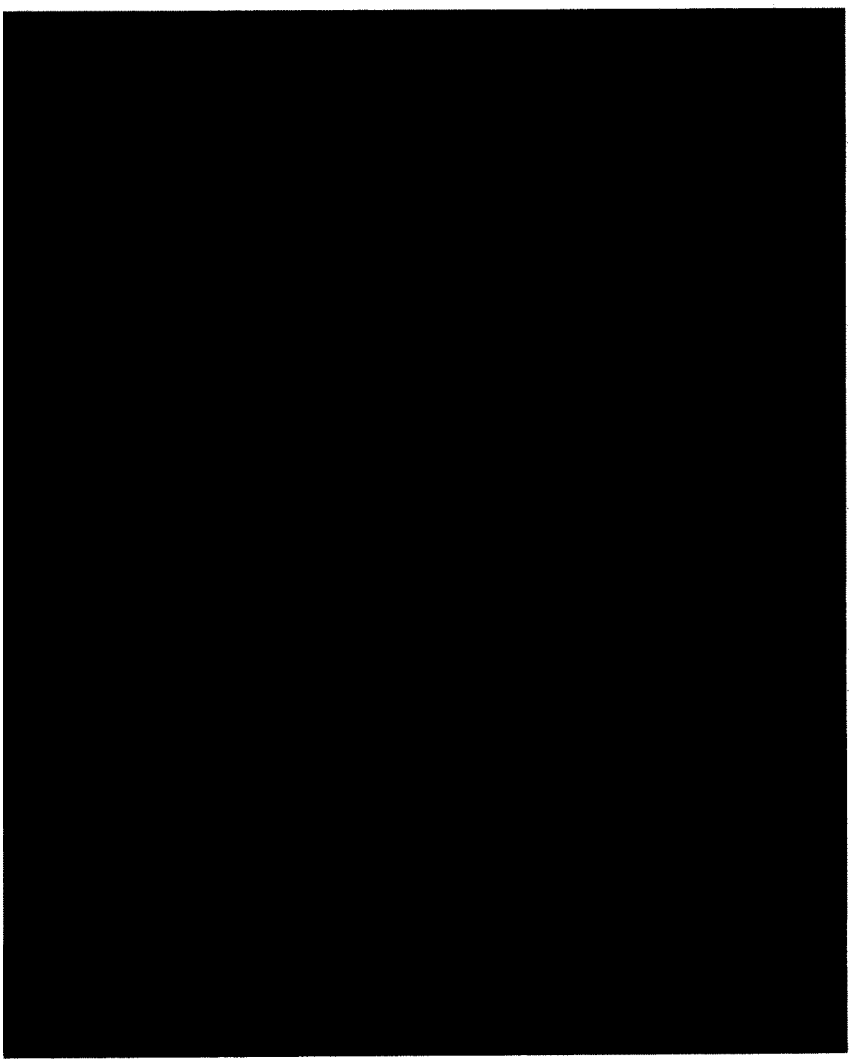


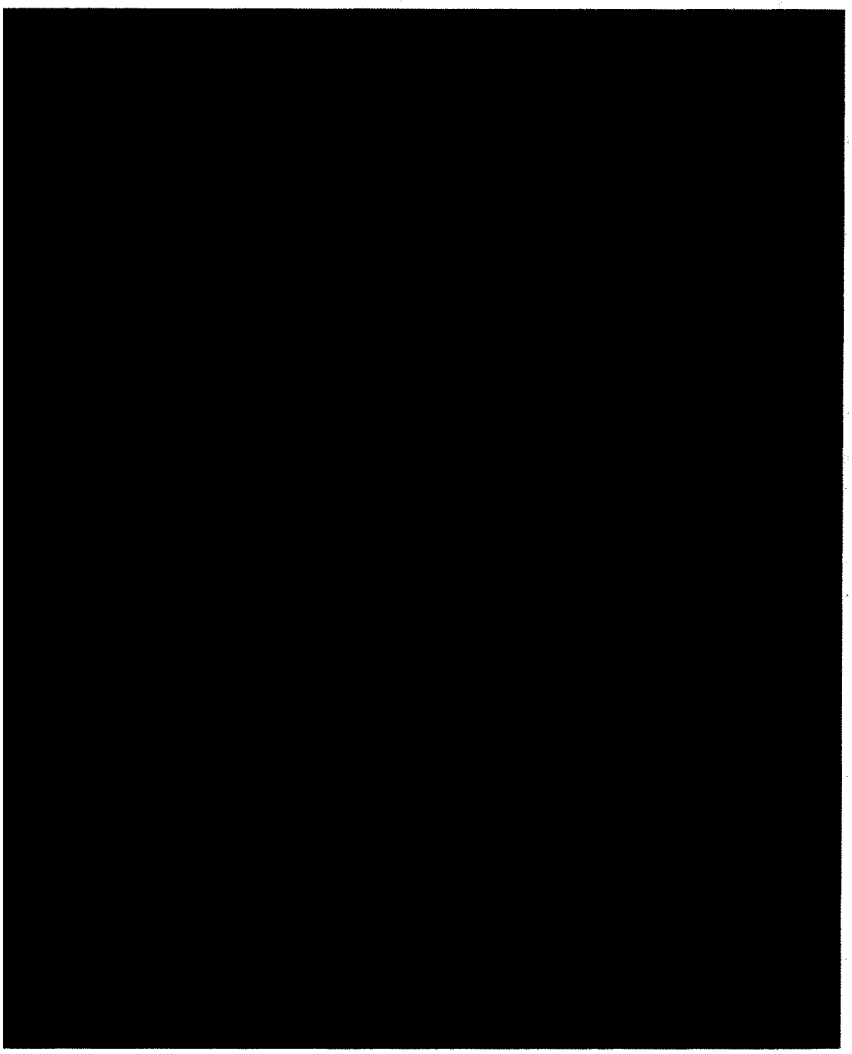


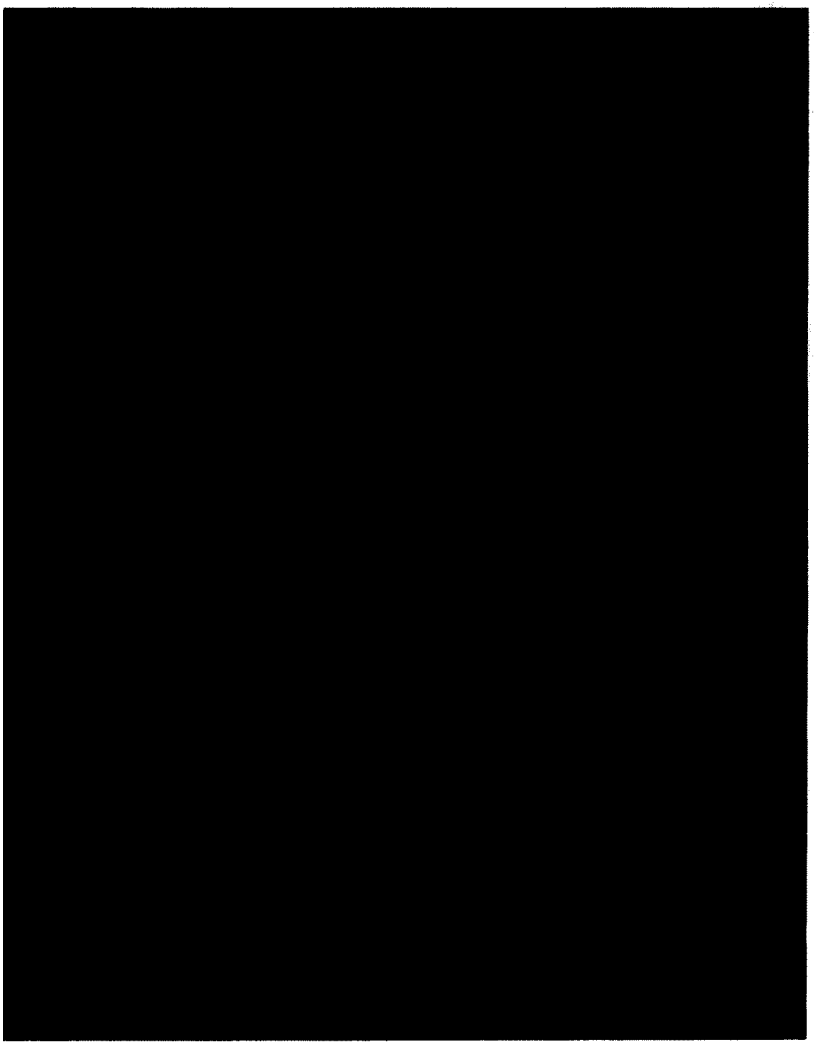
2 INTRODUCTION

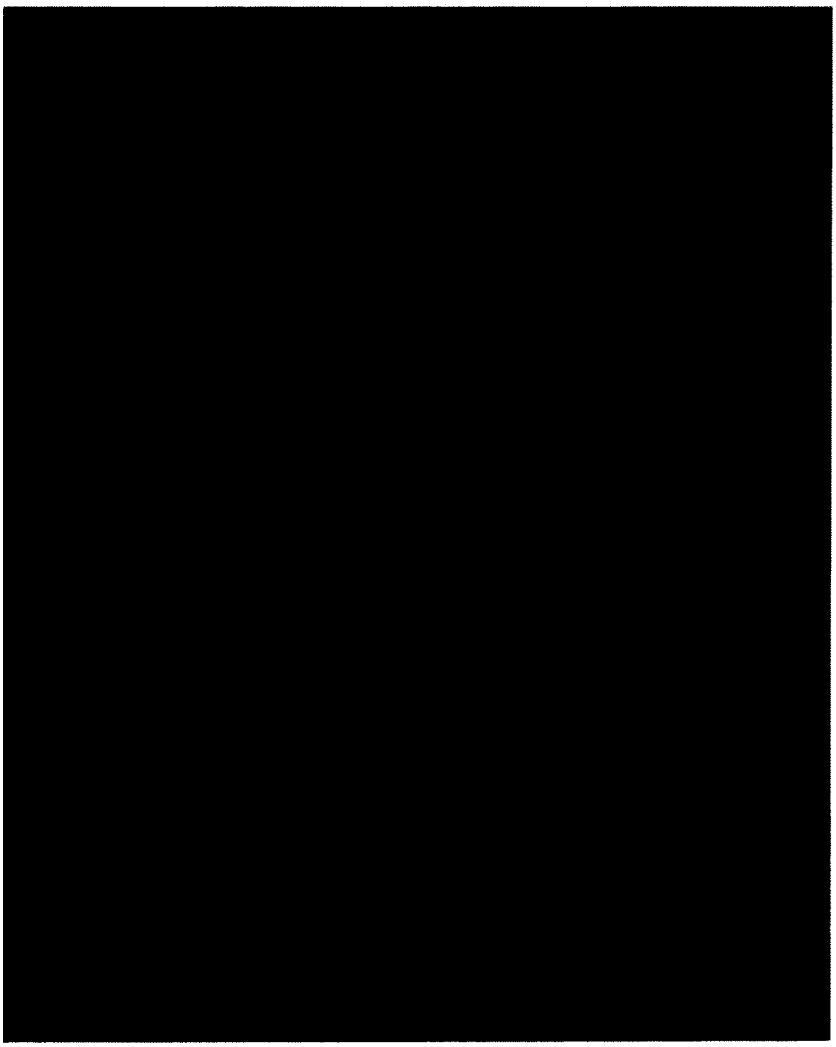


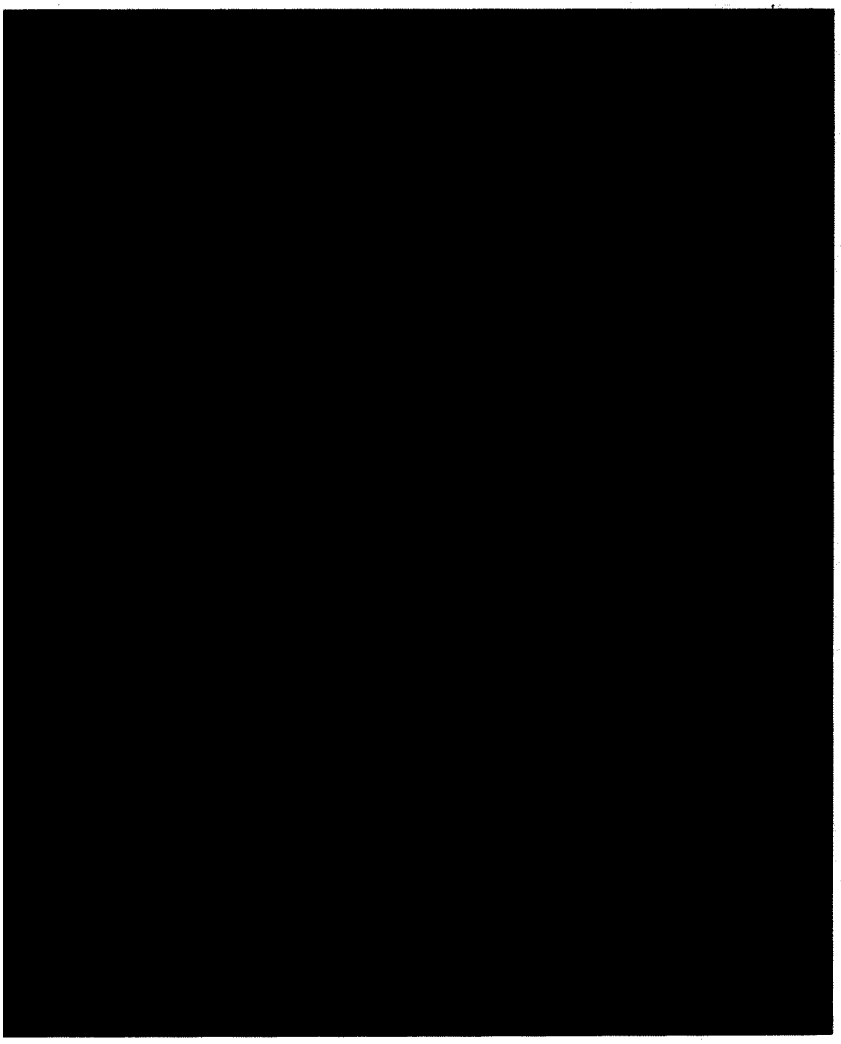


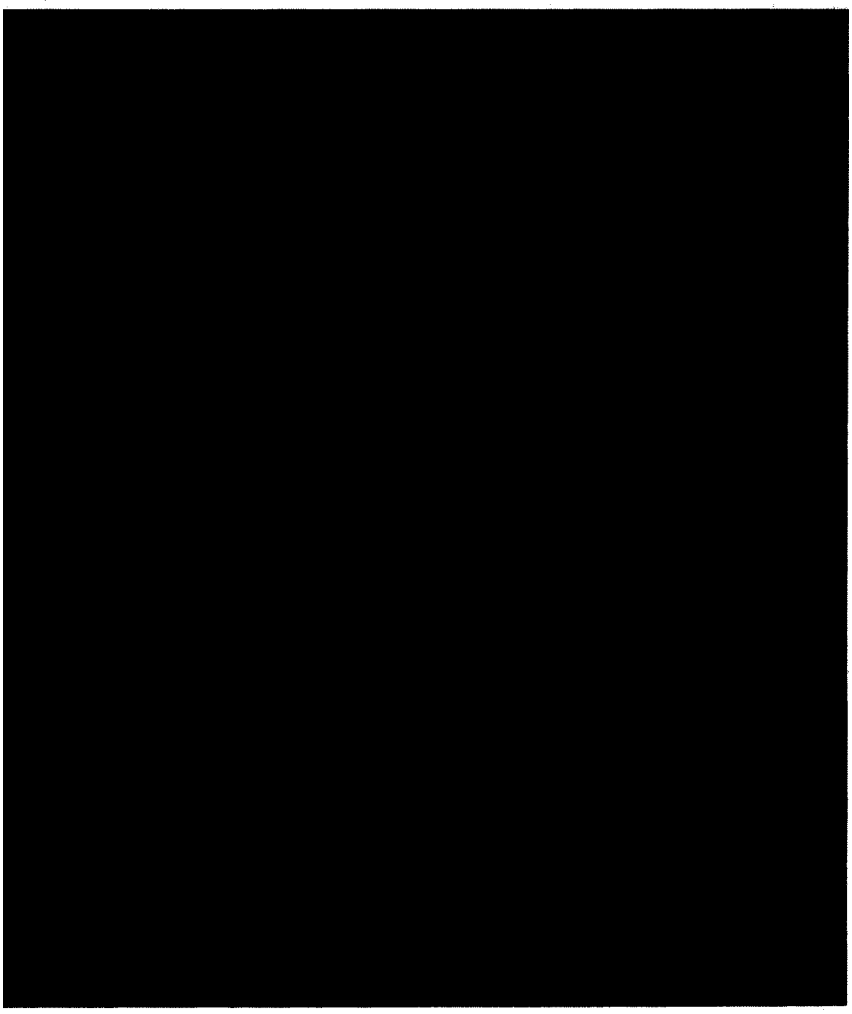


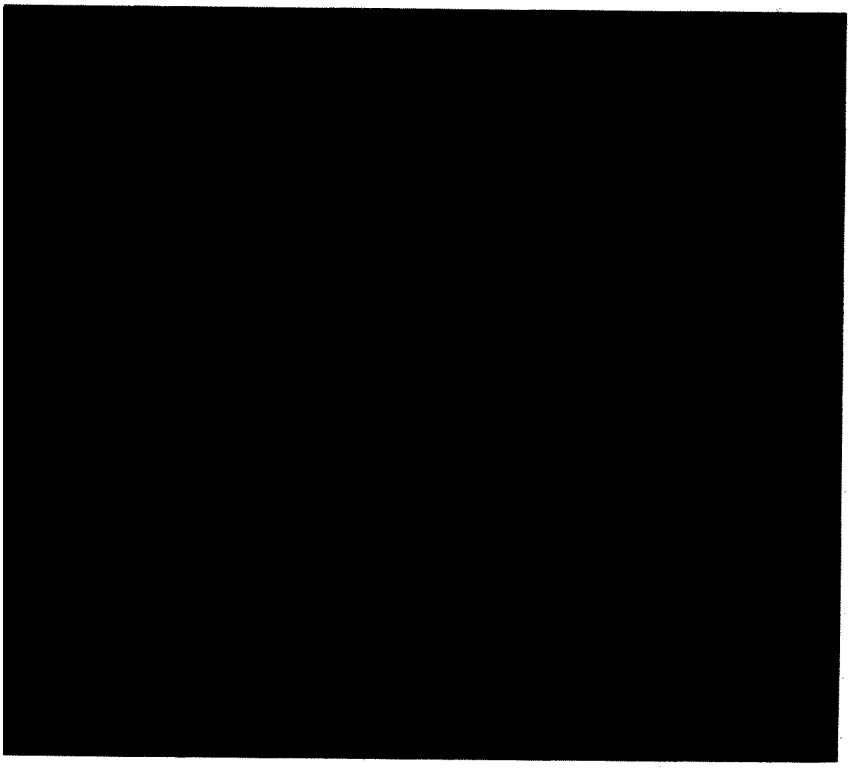












REDACTED BALANCE OF

PAGES 00797 – 00859

SENSITIVE SECURITY INFORMATION

Unknown

From: Couts, Todd (CMS/OIS)
Sent: Saturday, July 27, 2013 12:02 PM
To: 'lbjones[redacted]
Cc: Thompson, Tyrone (CMS/OIS); Holden, Stacey (CMS/OIS); Van, Hung B. (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Bing (CMS/OIS); Henry, Galina (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: Onsite at CGI
Attachments: Consolidated Tracking of Deployments

Lynn,

We would like to have you establish an on-site presence at CGI to be our eyes and ears. Right after our phone conversation Friday, Monique walked into my office and was having the same thoughts.

Your role is to be an independent source of truth from a governance perspective and to tell us what is really happening in terms of status/risks/progress, defects, artifact creation, etc. Peter Um, Hung, and Mark Oh are also spending more time at CGI to oversee the development itself. So, you are part of an on-site team.

We are assuming that two days per week would be sufficient to have insight while not getting in the way of work.

Please let me know if Tuesday and Thursday would work for you and what you need from us to make this happen.

Todd Couts
Centers for Medicare & Medicaid Services
Office of Info. Services | Consumer Info. & Insurance Systems Group
[redacted]

Unknown

From: Chao, Henry (CMS/OIS)

Sent: Saturday, July 20, 2013 7:55 AM

To: Cheryl Campbell; Bikram Bakshi; Chris Drumgoole; Par Rachakonda - US; Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Grothe, Kirk A. (CMS/OIS)

Cc: Karlton Kim; Laura Fasching; Calem, Mark (CGI Federal); Lakshmi Manambedu; M Finkel BB; Van, Hung B. (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Couts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rich Martin; Alan Koch; Geraldine Clawson; rich. schwarzkopf; gclawson[redacted] Ari Knausenberger; Radcliffe, Glenn D. (CMS/OIS); Joann Davis; 'Brian Paget'; Kash Badami; Thurston, Robert (CMS/CTR); Um, Peter (CMS/CTR); Igor Rafalovich; Riyaz Momin; Timothy Andrews; Mike Oelrich; Alicia Anderson; Stanley Rowen; Margush, Doug C. (CMS/OIS); Dill, Walter (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); Burke, Sheila M. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Adkins, Laura J. (CMS/OIS)

Subject: House Oversight and Government Reform Committee - Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus

Importance: High

Below are information and links to the Congressional Hearing Marilyn Tavenner and I attended this past Wednesday.

I am not sharing this with you because I think it's entertaining and informative. I wanted to share this with you so you can see and hear that both Marilyn and I under oath stated we are going to make October 1st. I would like you put yourself in my shoes standing before Congress, which in essence is standing before the American public, and know that you speak the tongue of not necessarily just past truths but the truth that you will make happen, the truth that is a promise to the public that millions of people depend on for us to make happen.

Aside from the political rhetoric, ranting, etc. my perspective is that on a personal and professional basis I made this promise on behalf of all of us and I have no doubt together we will drive the outcomes that flow from this promise.

Everyone in this email is a leader in this endeavor and I thank you for the support and vigilance in maintaining this promise that I speak of. I ask that you all take it every bit as serious as I do every minute of each day and in fact I will depend on it since much of my time going forward will be spent on Capitol Hill.

Please share this up, down, and wide so everyone will know not just what I promised on their behalf, but also to know that I am a true believer in our collective talents and commitment to change the world we live in and improve the lives of real people.

Thank you.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

The included link is to a C-SPAN video of the hearing.

http://www.c-spanvideo.org/program/CareInfor

House Oversight and Government Reform Committee

Wednesday July 17,2013 | 10:00 a.m. in 2154 Rayburn House Office Building

http://oversight.house.gov/hearing/evaluating-privacy-security-and-fraud-concerns-with-obamacares-information-sharing-apparatus/

Witnesses

The Honorable Danny Werfel

Principal Deputy Commissioner

Internal Revenue Service

The Honorable Marilyn B. Tavenner

Administrator

Centers for Medicare and Medicaid Services

U.S. Department of Health and Human Services

Mr. Henry Chao

Deputy Chief Information Officer

Deputy Director of the Office of Information Services

Centers for Medicare and Medicaid Services

U.S. Department of Health and Human Services

Mr. Alan R. Duncan

Assistant Inspector General for Security and Information Technology Services

Treasury Inspector General for Tax Administration

Unknown

From: Chao, Henry (CMS/OIS)
Sent: Tuesday, July 16, 2013 10:07 AM
To: Outerbridge, Monique (CMS/OIS)
Cc: Murray, Ruairi S. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Berkley, Katrina (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Subject: RE: CGI Monthly Meeting Next Week
Importance: High

Did you see my other email about first just talking to Rich Martin to convey just how low the confidence level and then pile on top of that the request for more money when we constantly struggle to get a release done, vacillating on delivery by due dates, and worse of all poor QA from build of the VMs all the way up to their software. They are the Prime and take direction from us so I don't want to hear about Marklogic, TMRK/URS, or anything elase. I just need to feel more confident they are not going to crash the plane at take-off, regardless of price.

Figure out how to get that conversation conducted and message conveyed.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Outerbridge, Monique (CMS/OIS)
Sent: Tuesday, July 16, 2013 10:02 AM
To: Robinson, Carolyn E. (CMS/OIS); Trenkle, Tony (CMS/OIS); King, Terris (CMS/OIS); Chao, Henry (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Cc: Shippy, Scott (CMS/OIS); Lewis, Melinda (CMS/OIS); Tierney, Janet L. (CMS/OIS); Blondell, Star (CMS/OIS); Weiss, Paul (CMS/OIS)
Subject: RE: CGI Monthly Meeting Next Week

I'm going to check with Mary to see if we can reschedule. Henry and I both will be in DC tomorrow and based on how Kirk looks and feels today I suspect he may not be in tomorrow.

From: Robinson, Carolyn E. (CMS/OIS)
Sent: Friday, July 12, 2013 12:11 PM
To: Trenkle, Tony (CMS/OIS); King, Terris (CMS/OIS); Chao, Henry (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Shippy, Scott (CMS/OIS); Lewis, Melinda (CMS/OIS); Tierney, Janet L. (CMS/OIS); Blondell, Star (CMS/OIS); Weiss, Paul (CMS/OIS)
Subject: CGI Monthly Meeting Next Week

There is a CGI monthly meeting next week. Some information you all will want to know is that they need about $38 million more to get them through Feb 2014. CIISG is reviewing the proposal, and they will be getting back, to Paul Weiss, by next Thursday. This $38 does not include the approximate $40 million we have in the budget for this contract.

Kirk, you will want to weigh in with any technical points you want to make.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

December 11, 2013

Mr. Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

Dear Mr. Chao:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, November 19, 2013, to testify at the hearing entitled "Security of HealthCare.gov."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

Also attached are Member requests made during the hearing. The format of your responses to these requests should follow the same format as your responses to the additional questions for the record.

To facilitate the printing of the hearing record, please respond to these questions and requests by the close of business on Tuesday, December 31, 2013. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@[redacted].

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachments

Henry Chao's Hearing
"HealthCare.gov"
Energy & Commerce Committee
Oversight & Investigations Subcommittee

November 19, 2013

Attachment 1—Additional Questions for the Record

The Honorable Cory Gardner

1. **Was there any consultation or recommendations from CMS to states on how to develop their websites?**

Answer: Section 1311 outlines Federal requirements for Marketplaces. These include the minimum functions the Marketplace must undertake as well as the oversight responsibilities the Marketplace must exercise in certifying and monitoring the performance of qualified health plans. Plans participating in the Marketplace must also comply with state insurance laws and Federal requirements in the Public Health Service Act. In defining the authority and duties of a Marketplace, states were required to incorporate, by reference or explicit provisions, the Federally-required Marketplace functions and oversight responsibilities as required by section 1321 of the Affordable Care Act.

2. **Do you know the extent of the interaction between CMS and Connect for Health Colorado?**

Answer: CMS is working with all states to continually improve their systems and business processes in accordance with published regulations and guidance. The foundation of the seamless consumer experience between state-based Marketplaces and Medicaid and CHIP agencies is formed through the development and use of a shared single eligibility system.

3. **To the best of your knowledge, have state websites been tested? If so, are they safe for the consumer?**

Answer: Yes, as part of each state's Blueprint submission, states had to both attest to, and submit test files to and receive files from the Data Services Hub. These included IT tests for functionality and compliance to established IT requirements. Tests included verification of compatible technology, infrastructure, and bandwidth required to support all Marketplace activities, as well as verification of a secure connection between the state system and the Data Services Hub. Tests were reviewed and confirmed to be effectively implemented by the independent verification and validation (IV&V) team through quality management processes and test procedures for Marketplace-development activities. Testing included verification of a secure connection between the state system and the Data Services Hub. A senior official in each state attested to their adherence to, and compliance with, the established security and privacy framework.

4. Were states able to utilize CMS' contractors to test their websites?

Answer: Each state-based Marketplace had its own vendor selection and IT development process separate from the contracting and IT development for the Federally-facilitated Marketplace.

5. Is Connect for Health Colorado fully functional?

Answer: Coloradans interested in what insurance options are available to them can browse plans directly through Connect for Health Colorado – Colorado's State-based Marketplace – If Coloradans are seeking financial assistance, they can apply in a coordinated, integrated application process that will result in an eligibility determination for any of the three affordability programs (advanced payment of the premium tax credits/cost sharing reductions, Medicaid or CHIP).

6. Has end-to-end testing been completed for state-run exchange websites?

Answer: As noted above, each state was required, as part of its Blueprint submission, to have a plan for testing their website, including the site's functionality. Marketplaces also must have capacity to accept and process applications online, compute APTCs, and process QHP selections and terminations electronically in coordination with issuers and CMS, among other Marketplace functions.

7. How has the connection between the state exchange and other databases, including federal databases, been tested for security and privacy?

Answer: In keeping with industry practice, CMS established strong security controls and standards, which each state was required to meet in order to connect to the Hub. These controls and standards are based on the guidelines issued by the National Institutes of Standards and Technology (NIST). Each state is required to establish a secure socket layer (SSL) connection between the state system and the Data Services Hub, to include FIPS 140-2 compliant encryption algorithms.

8. Are you confident the state sites do not present a risk?

Answer: States are required to meet the Blueprint requirements, pass functional and security testing, and sign a number of agreements attesting to the readiness and security of their IT system. Each state that was connected to the Hub on October 1 had either completed an authority to connect (ATC), or was granted a short-term ATC. Before an ATC is issued, states must sign a Computer Matching Agreement, an Interconnection Security Agreement and an Information Exchange Agreement, all of which bind the state to rules and operating procedures related to data security and privacy. Additionally, states are required to complete a security plan, a risk assessment, a corrective action plan to address risks, and a self-assessment or a third party test for each security control. Every state that was connected on October 1 adhered to these procedures.

The Honorable G.K. Butterfield

1. **The Hub and Marketplace systems have robust security systems designed to enable CMS to remain vigilant against any security threat.**

    a. **Can you provide some examples of instances which would cause CMS to take a closer look at a potential incident?**

Answer: Any unusual activity would cause CMS to examine an incident more closely.

    b. **Who would make the determination whether to initiate the Incident Response capability?**

Answer: The Incident Response (IR) process is activated every time an internal alert or external report of an event is triggered. The IR process includes the early workflow to triage all events and to place them into threat categories. Appropriate response processes are established for each threat category.

    c. **Would law enforcement authorities be notified automatically and in real time if the Incident Response capability was activated?**

Answer: If a violation of the law is suspected, the CMS security team notifies the Chief Information Security Officer of HHS, who in turn notifies the Office of Inspector General (OIG) Computer Crime Unit and also submits a report to the United States Computer Emergency Readiness Team (US CERT). Within CMS and HHS, the notification processes to these entities are automated to allow for rapid notification and response.

2. **Mr. Chao, you indicated that the issues that have delayed many of the 137,000 individuals in my district who are anxious to sign up for the ACA were due to an underestimation of the volume of users and in no way connected with security delays. It seems apparent that strong security safeguards are in place and that once the website is up and running our constituents can use it with confidence.**

    a. **With the Hub up and running as intended, can you explain why eastern North Carolinians should feel safe using it and what added efficiency and security benefits it provides?**

Answer: The security and protection of personal and financial information is a top priority for CMS, which, for decades, has protected the personal information Americans enrolled in Medicare, Medicaid, and CHIP. CMS used this experience and our security best practices to build a secure Data Services Hub that consumers should feel confident using.

CMS follows Federal law, government-wide security processes, and standard business practices to ensure stringent security and privacy protections. CMS' security protections are not singular in nature; rather the marketplace is protected by a vast array of security layers. First, the system was developed with secure code. Second, the system's infrastructure is physically and logically

protected by our hosting provider. Third, the system is protected through an internet defense shield in order to minimize access to any personal data. Finally, several entities provide direct and indirect security monitoring, security testing, and security oversight which include various organizational groups in CMS, HHS, US-CERT at the Department of Homeland Security (DHS), and the HHS OIG. Each of these groups have varying roles to ensure operational, management, and technical controls are implemented and successfully working. The Data Services Hub is protected by the high standards demanded of Federal information systems, including the standards prescribed by FISMA, NIST, the Privacy Act, and the Office of Management and Budget (OMB).

A large number of connections can cause security vulnerabilities. The Hub allows for one highly secured connection between closed databases of trusted states and Federal agencies instead of hundreds of connections. A series of business agreements enforce privacy controls between CMS and our Federal and state partners.

b. As the Marketplace interface comes online, can you discuss some of the security benefits that site provides to consumers, including the fact that they no longer need to provide detailed medical history?

Answer: HealthCare.gov does not collect personal health information (PHI). PHI is not necessary to the single streamlined application process because, due to the guaranteed issue provision of the Affordable Care Act, issuers are prohibited from denying applicants insurance based on their pre-existing conditions. Therefore, consumers in the Marketplace do not need to disclose details of their medical history as they might have had to do when they applied for health coverage in the past. Additionally, CMS follows Federal law, government-wide security processes, and standard business practices to ensure stringent security and privacy protections for the limited personal information provided in the single, streamlined application.

3. Both the data services Hub and the Federally-facilitated Marketplace eligibility and enrollment system build on existing information technology systems.

a. Can you explain how the Hub and Marketplace systems build on the security systems from programs like Medicare Advantage and State Medicaid agencies?

Answer: The Hub and Marketplace systems have the same stringent security standards that CMS has employed to protect other databases and information. CMS developed the Marketplace systems consistent with Federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS' systems of records are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002. These systems must also comply with various rules, regulations, and standards promulgated by HHS, OMB, DHS, and NIST.

4. It is clear that many existing laws, rules, regulations, and standards have been met for the Hub and Marketplace systems to operate. In other words, keeping sensitive information secure at HHS seems to be something your agency does in other areas.

a. Your agency has demonstrated before that it is able to effectively safeguard sensitive personal information from individuals, is that correct?

Answer: CMS has worked diligently over many years to protect the sensitive information we are tasked with maintaining as part of our services to millions of Americans. CMS operates and oversees systems that contain sensitive information about Medicare beneficiaries, physicians who participate in Medicare, and Medicare claims.

b. Can you provide example where HHS has managed an information technology system and protected sensitive personal information and compare that system to the Hub and Marketplace?

Answer: The Medicare program utilizes CMS' information systems to protect sensitive information about the Medicare beneficiaries, physicians who participate in Medicare, and Medicare claims. While the Hub and Marketplace serve a different population, our commitment to protect the private information of consumers, providers, and beneficiaries remains the same.

The Hub provides one highly secured connection among trusted Federal and state agencies instead of requiring each agency to set up what could have amounted to hundreds of independently established connections. Further, the Hub is not a database; it does not retain or store information. It is a routing tool that can validate applicant information from various trusted Government agencies through secure networks.

Attachment 2—Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record, and you indicated that you would provide that information. For your convenience, descriptions of the requested information are provided below.

The Honorable Michael C. Burgess

1. **Do you feel during your time that there has been a single implementation leader that you could look to for advice and direction throughout this process? If so, please provide their name(s).**

Answer: As Administrator of CMS, Marilyn Tavenner oversees Affordable Care Act implementation.

The Honorable Gregg Harper

1. **Do you have a central reporting location of the navigators that are in violation or reported in violation?**

Answer: The Navigator program and grantees are overseen by the Center for Consumer Information and Insurance Oversight and by the Office of Acquisition and Grants Management, which ensure that all grantees abide by the terms of their funding agreements.

CMS has several tools to respond to any organizations found in violation of the terms of the Federal Navigator program, including issuing a Corrective Action Plan to the grantee, decertifying individual Navigators, and terminating the grant.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

December 11, 2013

Mr. Jason Providakes
Senior Vice President and General Manager
Center for Connected Government
MITRE Corporation
7515 Colshire Drive
McLean, VA 22102-7539

Dear Mr. Providakes:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, November 19, 2013, to testify at the hearing entitled "Security of HealthCare.gov."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, December 31, 2013. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@[redacted].

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

For the Record: Responses to Additional Questions from The Honorable G.K. Butterfield regarding testimony at Energy & Commerce Oversight & Investigations Subcommittee hearing Nov. 19, 2013 of:

Dr. Jason Providakes
Senior Vice President
Center for Connected Government
The MITRE Corporation

1). Can you elaborate on the successes MITRE had in remediating risks assessed as "high" with CMS-designated contractors?

Dr. Providakes:
MITRE has no role in the remediation of risks. MITRE does not remediate findings. We recommend mitigations. It is the responsibility of CMS and its contractors to correct any risks identified during a Security Control Assessment (SCA). MITRE may, at the request of CMS, go back and validate that previously identified risks have been remediated.

Two high risk vulnerabilities were identified as unresolved in the Exchange Consumer Web Services (ECWS) Final Security Control Assessment (SCA) Report dated August 23, 2013. MITRE was not requested by CMS to validate closure of these risks and therefore MITRE has no knowledge of the status of these risks. Those two risks were:

Inconsistent use of security communication protocols: The use of secure computer communications (in the form of encryption standards found in Hyper Text Transport Protocol Secure (HTTPS)) to transport data between the user and the ECWS application was found to be inconsistent, thereby potentially exposing data in transit. MITRE observed that data traffic was sent using an unsecured transport protocol rather than HTTPS encryption.

Several components were not production ready, and MITRE was therefore unable to test some CMS security controls, e.g. Access Control: Several components (e.g., LDAP; Splunk) were not production ready, which meant that MITRE was unable to assess the degree to which certain CMS mandated security controls had been implemented. These limitations were specifically documented in the ECWS SCA Final Report.

2.) Can you discuss some of the security progress that MITRE observed through subsequent SCAs?

Dr. Providakes: MITRE has not been involved in any Healthcare.gov SCAs since the 11 October 11, SCA – "Health Insurance eXchange (HIX) August-September 2013 SCA Report." MITRE is currently conducting an onsite application-only SCA on the Federal Facilitated Marketplace system. The expected completion date is January 9, 2014.

3.) Has CMS outlined a timetable to meet additional outstanding risks identified by MITRE in SCA reports?

Dr. Providakes: MITRE is not aware of any timetable regarding the mitigation of any outstanding risks associated with Healthcare.gov. CMS, in conjunction with its contractors, is responsible for the development and maintenance of the Plan of Action and Milestone (POAM) for remediation of security risks. MITRE has no involvement with POAMs and/or timetables.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

December 11, 2013

Ms. Maggie Bauer
Senior Vice President
Health Services
Creative Computing Solutions, Inc.
1901 Research Boulevard, Suite 600
Rockville, MD 20850

Dear Ms. Bauer:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, November 19, 2013, to testify at the hearing entitled "Security of HealthCare.gov."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

Also attached are Member requests made during the hearing. The format of your responses to these requests should follow the same format as your responses to the additional questions for the record.

To facilitate the printing of the hearing record, please respond to these questions and requests by the close of business on Tuesday, December 31, 2013. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens@[redacted]

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachments

1001 Pennsylvania Avenue, NW, Washington, DC 20004-2595 ▪ p 202 624-2500 ▪ f 202 628-5116

crowell moring

Michael Gill
(202) 508-8843
mgill@crowell.com

December 23, 2013

The Honorable Tim Murphy
Chairman
House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
2125 Rayburn House Office Building
Washington, D.C. 20515-6115

Re: Response to Questions for the Record from Creative Computing Solutions, Inc.

Dear Mr. Chairman:

On behalf of our client, Creative Computing Solutions, Inc. ("CCSi"), we are pleased to provide the attached responses to the Subcommittee's Questions for the Record letter.

Sincerely,

Michael Gill
Counsel for CCSi

cc: The Honorable Diana DeGette, Ranking Minority Member

Attachment 1 — Additional Questions for the Record

The Honorable G.K. Butterfield

It is clear that CMS has a robust framework to respond to malicious activity that CCSi adheres to.

a. **Ms. Bauer, does CCSi use both automated and manual approaches to search for malicious behavior?**

Answer: Yes.

b. **Can you provide an example of an anomaly that might prompt CCSi to respond?**

Answer: A foreign (non U.S.) IP address attempting to connect to healthcare.gov.

c. **Would CCSi implement the CMS approved Incident Response Plan (IRP) if any anomaly related to sensitive information was detected?**

Answer: Yes.

d. **At what point might law enforcement be involved under the IRP?**

Answer: CMS would make any decisions to involve law enforcement.

Attachment 2-Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record, and you indicated that you would provide that information. For your convenience, descriptions of the requested information are provided below.

The Honorable Tim Murphy

a. **During the hearing, we asked Mr. Amsler if he had all of the tools and capabilities to successfully and fully monitor the system, he said that "there are some things that we have asked for that are not in place as of yet." You said you agreed with his statement. Please elaborate on why you agree with that statement and how it applies to CCSi.**

Answer: Today's cyber security environment involves constantly evolving threats and equally evolving tools, technologies and techniques to address them. CCSi's objective is to recommend and implement the most robust security approaches for our clients. Those recommendations will evolve and change over time to reflect the current threat environment. Over the course of its contracts, CCSi normally requests additional capabilities to service the client and address the current threat environment. To this end, CCSi along with its subcontractor, compiled a list of additional, potential security measures for CMS to consider.

December 11, 2013

Mr. David Amsler
President and CIO
Foreground Security Inc.
801 International Parkway
5th Floor
Lake Mary, FL 32746

Dear Mr. Amsler:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, November 19, 2013, to testify at the hearing entitled "Security of HealthCare.gov."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

Also attached are Member requests made during the hearing. The format of your responses to these requests should follow the same format as your responses to the additional questions for the record.

To facilitate the printing of the hearing record, please respond to these questions and requests by the close of business on Tuesday, December 31, 2013. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to brittany.havens[redacted].

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachments

David Amsler
President and CIO
Security and Healthcare.gov

Attachment 1- Additional Questions for the Record

The Honorable G.K. Butterfield

1. It is encouraging to know that numerous highly trained security personnel are continuously monitoring the new virtual data center created for the ACA
    a. Mr. Amsler, does Foreground Security use both automated and manual approaches to search for malicious behavior?

Foreground Security uses a variety of tools to examine network, server, and application activity for matches to known malicious behavior and/or deviations from "normal" user behavior. Through these pattern matching and anomaly detection functions, these tools provide an automated mechanism for identifying malicious behaviors.

Our human analysts review the logs and alerts generated by these tools to differentiate between normal activity that may have triggered an alert and truly malicious behavior. The team also analyzes raw data generated by the healthcare.gov systems and networks to identify malicious behavior the tools may not be capable of detecting. This is a key function, as sophisticated attackers will often change their tactics to avoid automated detection.

    b. If malicious activity is detected, what responsibilities does Foreground Security have to report that activity and who do you report it to?

If malicious activity is detected, our procedures dictate that we gather all relevant details including systems affected, functions and data within those systems that may have been exposed, the nature of the activity in question, users and external systems involved, timeline of events, and other information that helps determine the scope of the incident.

Our team then opens an internal CMS incident case, populates it with those key details, and escalates to the Federal IT Security Manager on duty. Depending on the criticality of the incident, that escalation occurs in as little as 30 minutes and may also include the Director for Marketplace Security, the CMS Chief Information Security Officer (CISO), and other CMS and HHS executive leadership.

c. At what point might law enforcement become involved after malicious activity has been noticed?

Our incident reporting chain includes the HHS Office of the Inspector General (OIG), which provides criminal investigative functions and acts as an interface to other Law Enforcement agencies in cases where an incident is determined to include unlawful activities. That determination is made by the OIG in conjunction with the FBI and other Law Enforcement agencies with whom the OIG liaises.

Attachment 2- Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record, and you indicated that you would provide that information. For your convenience, descriptions of the requested information are provided below

The Honorable Tim Murphy

During the hearing, when asked if you have all of the tools and capabilities to successfully and fully monitor the system you said that "there are some things that we have asked for that are not in place as of yet." Please elaborate on what you meant when you said that.

1. Foreground and our partner CCSi maintain a complete list of current capabilities, required tools/capabilities that aren't in place or functioning, and future roadmap items that are requested. That report is provided to the government (COTR and COR) on a monthly basis and I believe examples of that report were turned over to the committee during our extensive document collection effort that included every email, report, or all other documents related to this contract.